الجمهورية العربية السورية

جـامعة تشـرين

كليـة الهندسـة الميكانيكيةو الكهربائيـة

مراقبة وتحليل بارامترات أمن الشبكات الحاسوبية اللاسلكية

WLAN Security Parameters Monitoring & Analyzing

رسالة أعدت لنيل درجة الماجستير في هندسة الاتصالات المعلوماتية Tempus

إعداد المهندس

زياد شيخ ياسين

إشـــراف

الدكتور رياض ضاهر

أستاذ مساعد في قسم هندسة الحاسبات و التحكم الآلي

كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين

الدكتور محمد حجازية

مدرس في قسم هندسة الحاسبات و التحكم الآلي

كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين

اللاذقـيـة ٢٠١١

الفهرس

الموضوع	رقم الصفحة
مقدمة	
الفصل الأول: أساسيات الشبكات الحاسوبية اللاسلكية	**٦**
١-١ معايير الشبكات اللاسلكية 802.11	٦
١-٢ طوبولوجيا المعيار ٨٠٢,١١	١٠
١-٣ طريقة عمل الشبكة الحاسوبية اللاسلكية	١٢
١-٤ بنية الإطارات اللاسلكية	١٣
١-٥ تحليل الإطارات اللاسلكية	١٥
١-٦ بروتوكولات نقل البيانات TCP/UDP	١٦
الفصل الثاني: نظام أمن الشبكات الحاسوبية اللاسلكية	**١٩**
٢-١ بروتوكولات أمن الشبكات اللاسلكية	١٩
٢-٢ الأمن عبر طبقات الشبكات اللاسلكية	٢٤
٢-٣ المصادقة والترابط في الشبكات اللاسلكية	٢٨
٢-٤ تحسين أمن الشبكات الحاسوبية اللاسلكية	٣٠
الفصل الثالث: الهجمات والتهديدات في الشبكات الحاسوبية اللاسلكية	**٣٦**
٣-١ أدوات وطرق اختراق الشبكات الحاسوبية اللاسلكية	٣٦
٣-٢ تصنيف الهجمات في الشبكات الحاسوبية اللاسلكية	٣٧
٣-٣ نظام تتبع الدخلاء WLAN/ IDS	٤٠

الفصل الرابع : تحليل التشكيلات الأمنية للشبكات WLAN **٤٢**

٤ ـ١ تحليل أمن الشبكات الحاسوبية اللاسلكية ٤٢

٤–٢ الأدوات المستخدمة للمراقبة والتحليل ٥٠

الفصل الخامس : القياسات و النتائج **٥٤**

السيناريوهات المقترحة وكيفية إجراء التجارب والنتائج المستخلصة ٥٤

الملحق رقم ١: جدول المصطلحات المستخدمة ٧٦

الملحق رقم ٢: جدول بالمختصرات المستخدمة ٧٧

الملحق رقم ٣: جزء من الكود البرمجي لبرنامج تجميع النتائج ٧٨

الملحق رقم ٤ : المراجع العربية و الأجنبية ٨٣

مقدمة

انتشرت الشبكات اللاسلكية WLAN في الأونة الأخيرة على نطاق واسع في الشركات والمؤسسات والمستشفيات والمطارات وغيرها وتعزى جاذبية الشبكات WLAN الى المواصفات والمميزات التي يمكن تلخيصها بتأمينها أجواء مفتوحة للإرسال ، بحيث يتحرر المستخدم من قيود الأسلاك أو الوسائط المعتادة . وبذلك تتاح له حرية الحركة من مكان إلى آخر مع تأمين الاتصال بالشبكة .

إن الأجواء المفتوحة التي تتيحها الشبكات WLAN هي ميزة بالنسبة للمستعمل لكنها بالمقابل تشكل ثغرة يمكن النفاذ منها إلى نظام الشبكة للعبث بها أو بمواردها وتعريض نظامها الأمني للخطر .

بناء على ماسبق يكتسب نظام أمن وحماية الشبكات WLAN أهمية خاصة ويمكن الإطلاع على تقرير معهد أمن الحاسوب ومكتب التحقيقات الفدرالي الأمريكي عام ٢٠٠٩ والذي بين فيه أن ٣٠% من الجهات التي شملتها الدراسة ، أفادت أن شبكاتها الحاسوبية اللاسلكية تعرضت إلى هجمات وا ٕن مانسبته %(50-40) من الشبكات تتميز بمستوى حماية ضعيف أولايوجد أي نوع من الحماية على الإطلاق [1].

يتم الهجوم على الشبكات WLAN من قبل مجموعة من الهواة أو المحترفين أو الفضوليين وغيرهم ويمكن استخدام أدوات وبرامج بسيطة أو معقدة ، وغالبا ماتكون هذه الأدوات متاحة بأسعار وكلف رخيصة .

تتعرض الشبكات WLAN الى انواع عديدة من الهجمات ناتجة إما عن الثغرات الأمنية الحاصلة أثناء التركيب أو ضعف البروتوكولات الأمنية أو استثمار النطاق الترددي للإرسال .

لكن بالمقابل يتوفر هناك مجموعة من وسائل الحماية لأنظمة الشبكات WLAN تبدأ بتحديد سياسات أمنية احترازية وبناء آلية مناسبة لهذه السياسات وكذلك ضمان تركيب وا ٕدارة هذه الشبكات من قبل أناس متخصصين مع مراقبة الشبكة والأنشطة المشبوهة باستمرار مع اتخاذ الحيطة لحسن اختيار اماكن توضع التجهيزات الشبكية واستخدام بروتوكولات أمنية مناسبة بما فيها تلك المعتمدة على أنظمة التشفير المناسبة

يقترح البحث مجموعة من السيناريوهات الأمنية المعتمدة على نمط تشغيل البنية التحتية الموافق لبارامترات أمنية مختلفة وتمت دراسة هذه البارامترات والتوصل إلى مجموعة من النتائج وصو لا إلى رفع مجموعة من التوصيات بهذا الخصوص

وتأتي الدراسة في خمسة فصول هي:

- أساسيات الشبكات الحاسوبية اللاسلكية
- نظام أمن الشبكات الحاسوبية اللاسلكية
- الاختراقات والهجمات في الشبكات الحاسوبية اللاسلكية
- تحليل أمن الشبكات الحاسوبية اللاسلكية
- القياسات و النتائج

كما يوجد أربعة ملاحق هي:

- الملحق رقم واحد جدول بأهم المصطلحات المستخدمة في الدراسة.

- الملحق رقم إثنان جدول بالمختصرات المستخدمة في الدراسة .
- الملحق رقم ثلاثة يبن جزء من الكود البرمجي لبرنامج تجميع النتائج
- الملحق رقم أربعة عبارة عن قائمة بالكتب و المراجع العربية و الأجنبية التي تم الإستعانة بها.

راجياً أن تساهم هذه الدراسة في في اضافة ما للبحوث المتعلقة بهذا الموضوعو أن تكون هناك دراسات لاحقة مكملة في هذا المجال ،كما لا يسعني إلا أن أتقدم بالشكر إلى كل من قدم لي المساعدة في إتمام هذه الدراسة وأخص بالشكرالدكتور رياض ضاهر والدكتور محمد حجازية لما قدماه لي من نصح وتوجيهات ومساعدة.

والله وليٌ التوفيق

الفصل الأول

أساسيات الشبكات الحاسوبية اللاسلكية
WLAN Basics

مقدمة :

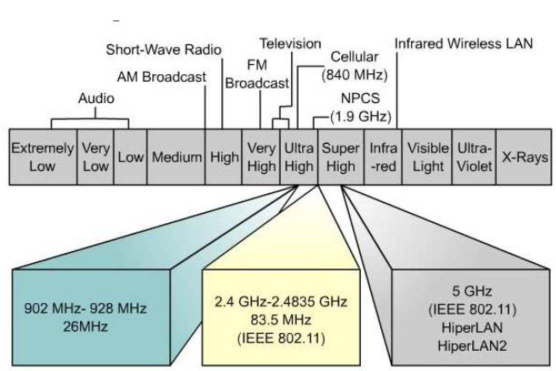
يتطرق هذا الفصل إلى الشبكات اللاسلكية WLANومعاييرها وطرق تشبيكها وبنيتها الطبقية بالتوافق مع معمارية النموذج المفتوح OSI وتركز الدراسة على الشبكات الحاسوبية اللاسلكية WLAN ونماذجها وطرق وصلها وآلية عمل الشبكات الحاسوبية اللاسلكية وطرق اتصال الزبون بنقطة الوصول .

١-١ معايير الشبكات اللاسلكية Wireless Standards

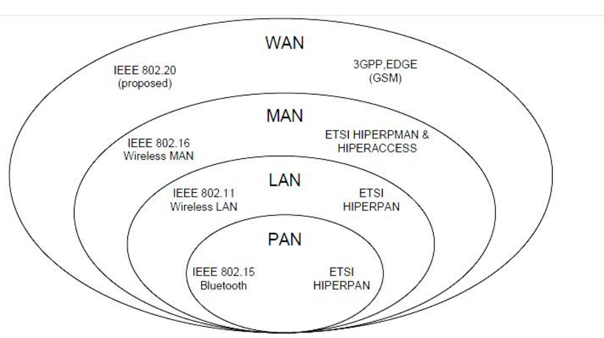
اطلق المعهد الأمريكي IEEE مشروعا شهيرا سمي IEEE 802 ، والمقتبس اسمه من العام ١٩٨٠ وشهر شباط على إصدار معيار مماثل تحت رقم ITU٨٨٠٢ [13]
انصب اهتمام لجان المشروع IEEE802 على تحديد المواصفات القياسية للمجالات المتصلة بمتطلبات الشبكات المحلية والمتوسطة ومن هذه المجالات :

١. معايير ومواصفات أوساط الإرسال المستخدمة في الشبكة
٢. مواصفات وخصائص الإشارات والجهود الكهربائية المستخدمة
٣. مواصفات الرزم والإطارات المتبادلة عبر الشبكة
٤. الطوبولجيات الممكنة وتحديد الخصائص لكل طوبولوجية
٥. بروتوكولات الاتصال بين أجهزة الشبكة
٦. بروتوكولات النفاذ إلى الشبكة من أجهزة المستعملين

اقترحت لجان المشروع IEEE802 مجموعة من المعايير خاصة بالشبكات المحلية والمتوسطة اسندت لها عام IEEE802 مع تمييزها برقم مفصول بنقطة .



الشكل (١-١) يبين موقع الشبكات اللاسلكية في المجال الترددي



الشكل (١-٢) بين معايير الشبكات اللاسلكية

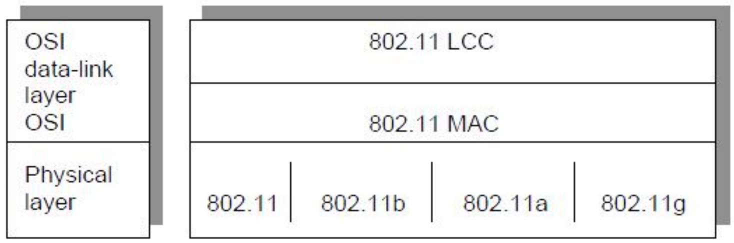
نلاحظ من الشكلين (١-١) و(١-٢) ان هناك مجموعة من معايير الشبكات اللاسلكية منها الشيكات الشخصية PAN والشبكات الحاسوبية اللاسلكية WLAN وشبكات المدن WMANوالشبكات الواسعة WWAN وهو معيارمقترح والجدول التالي يبين عائلة معايير 802 :

المعيار	الوصف
802.1	معايير ربط الشبكات بعضها ببعض المتعلقة بإدارة الشبكة
802.2	تعرف المعيار العام للطبقة الفرعية LLC
802.3	معيار الاثرنت ، تعرف الطبقة الفرعية MAC للشبكة بالممر العام والمستخدمة للبروتوكول CSMA/CD
802.4	تعرف الطبقة الفرعية MAC للشبكة بالممر العام والتي تعمل طريقة تمرير العلام
802.5	تعرف الطبقة الفرعية MAC للشبكة الحلقية
802.6	معيار يخص الشبكات المتوسطة MAN
802.7	تعرف معايير الشبكات عريضة الحزمة Broadband
802.8	ميار استخدام الألياف الضوئية كخطوط اتصال في الشبكات المحلية
802.9	معيار ارسال البيانات والمعلومات الصوتية في الشبكات المحلية وربطها مع شبكة ISDN
802.10	الشبكات المحلية الافتراضية
802.11	معايير الشبكات المحلية اللاسلكية
802.12	يعرف النفاذ الى الشبكة المحلية بأفضلية عند الطلب
802.13	غير مستعمل
802.14	يعرف معايير مودم الكبل
802.15	الشبكات اللاسلكية الشخصية WPAN
802.16	معايير اللاسلكي عريض الحزمة
802.17	حلقة الباكيت المرن
802.18	IEEE 802.18 Radio Regulatory TAG
٨٠٢,١٩	IEEE 802.19 Coexistence TAG
802.20	شبكة الوصول اللاسلكي العريضة المتنقلة IEEE 802.20 Mobile Broadband Wireless Access
802.21	IEEE 802.21 Media Independent Handoff التجول المستقل عن الوسط
802.22	شبكة اللاسلكي الاقليمية
802.23	Emergency Services Working Group مجموعة خدمات عمل الطوارئ

الجدول (١-١) يبن عائلة المعايير 802.11

تم إقرار المعيار 802.11 في حزيران ١٩٩٧ وهذا المعيار يتضمن مجموعة من الخصائص للشبكات اللاسلكية والتي تستخدم في المجال الصناعي والعلمي والطبي .

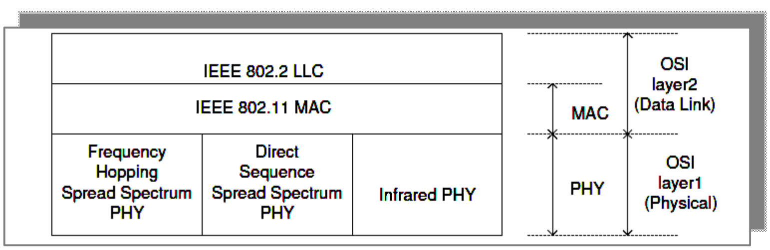
يعمل هذا المعيار في الطبقات السفلى من النموذج OSI المرجعي كما هو مبين في الشكل (١-٣) ان عنوان البروتوكول وطبقة MACو الطبقة الفيزيائية PHY هي طبقات مستقلة ، وتعمل طبقة التحكم بالوصول MAC لنقل المعلومات بين الوسط الفيزيائي وتعمل طبقة وصل البيانات[18] وهذا مبين في الشكل(١-١) :



الشكل (١-٣) يبن بنية طبقات المعيار 802.11 بالمقارنة مع طبقات OSI [1]

١-١-١ الطبقة الفيزيائية PHY :

يعود للطبقةالفيزيائية مسؤولية إقامة الإتصال او إنهائه ، وتعمل مع أجهزة متكافئة ومشتركة بوسط الإتصال ، وتجهز الطبقة البيانات الأولية للإرسال عبر المجال اللاسلكي وكذلك تتلقى البيانات الأولية من لمجال اللاسلكي وتجهيزها للتمرير إلى الطبقة MAC ، تقسم الطبقة الفيزيائية منطقياً إلى طبقتين فرعيتين بشكل مشابه للإثرنت



الشكل (١-٤) يبن مكونات طبقتي PHY, MAC في معيار 802.11 [1]

- الطبقة الفرعية PMD (Physical Medium Dependent)
- الطبقة الفرعية PLC (PhysicalLayer Convergence)

تتواصل الطبقة MAC مع الطبقة الفرعية PLC من خلال نقاط SAP PHY ، حيث تستقبل PLC الرزم MPDUs ، وترسلها بعد إلحاق حقول معلومات للرزم ، تستعمل في الطبقة الفيزيائية والمستقبل ، كذلك تمرر الإطارات القادمة من وسط الإرسال نحو طبقة MAC ومن الجدير بالذكر أنه يوجد نوع PLC لكل طبقة فيزيائية من الطبقات الثلاث FHSS,DSSS,IR

تعمل الطبقة الفرعية PMD بتوجيهات الطبقة PLC بإنجاز الإرسال والإستقبال الفعلي لمكونات الطبقة الفيزيائية بين المحطات عبر الوسط اللاسلكي . إن الطبقتين PMD وPLC تتواصلان بواسطة التعليمات البدائية للسيطرة على عملية الإرسال والإستقبال

تلعب الطبقة الفيزيائية دورا حيوياً في تحديد خصائص الاتصال ويتعلق ذلك بتعريف النطاق الترددي ، وتقنيات التعديل أو الترميز المستخدمة والتي ستلعب دوراً حاسماً في تحديد عرض الحزمة وسرعة نقل البيانات فكلما كانت البيانات مرمزة بفاعلية أكثر كلما زادت سرعة نقل البيانات التي يمكن تحقيقها ولكن ذلك يتطلب استخدم تقانات ترميز فعالة ، وتحقيقها بواسطة تجهيزات متطورة قادرة على ترميز وفك ترميز البيانات بالسرعة المطلوبة .

١-١-٢ وظائف الطبقة MAC

تحدد طبقة التحكم بالوصول إلى الوسط MAC طريقة الوصول إلى الناقل بإسلوب يشبه معيار الإثرنت 802.3 مع التكيف في الوظائف الخاصة بإرسال الإشارات اللاسلكية باعتبار أن نسبة الخطأ في هذه الحالة ، أعلى من تلك الموجودة في الأوساط السلكية .تزود طبقة MAC بالموثوقية لإرسال البيانات بشكل مشابه للشبكات السلكية ولتحقيق ذلك تقوم بثلاث وظائف :

١. تنفيذ بروتوكول يضمن موثوقية البيانات المرسلة
٢. تنفيذ بروتوكول للوصول المشترك لوسط الإرسال بين مجموعة مستخدمين .
٣. تنفيذ بروتوكول لحماية البيانات المرسلة

ترسل بيانات المستخدم إلى نقطة الوصول ، ولضمان وصول الإطارات بشكل موثوق يتم تلقي إقرارايجابي فوري من نقطة النفاذ وبعد مرور فاصل زمني محدد يعمل جهاو الإرسال (الزبون) على إعادة إرسال الإطار .
ويتم ضمان الوصول المشترك لجميع الزبائن من خلال آليتين :

- ❒ وظيفة التنسيق الموزع DCF (Distributed Coordination Function)
- ❒ وظيفة التنسيق المركزي PCF (Point Coordination Function)

إن وظيفة وحدة التنسيق الموزع تتيح ضبط تحسس الحامل فيزيائياً وافتراضياً . يتم الضبط الفيزيائي من خلال بروتوكول يناسب الإرسال اللاسلكي . وهو بروتوكول تعدد الوصول مع تحسس الحامل ولكن مع تجنب التصادم CSMA/CA ويعمل البروتوكول على تخفيف التصادم من خلال بيان فيما إذا كان الوسط اللاسلكي شاغراً أم لا وينصح محطة الزبون الاستماع قبل الإرسال ، وفي حالة الإرسال أثناء انشغال الوسط يستدرك ذلك من خلال خوارزمية التراجع الأسي .
أما وظيفة التنسيق المركزي PCF تقيم آلية المنسق في نقطة الوصول AP ، وتستعمل لتحديد المحطة التي يمكنها أن ترسل ، من ضمن مجموعة المحطات ، عن طريق لائحة مختارة .

١-٢ طبولوجيا المعيار IEEE 802.11

يعرف معيار 802.11 نموذجين للربط هما :

❶ **نموذج البنية التحتية Infrastructure mode**

❷ **نموذج الشبكة المتكافئة Ad hoc mode**

١- نموذج البنية التحتية Infrastructure mode

يتضمن نموذج البنية التحتية نقطة وصول واحدة على الأقل متصلة ببنية سلكية من جهة ومجموعة من المحطات اللاسلكية وهذه البنية تدعى بـ (BSS) Basic Service Set الشكل (١-٥)



الشكل (١-٥) يبين نمط البنية التحتية

وعندما ترغب إحدى المحطات أن تتصل بالأخرى يجب ان تمر العملية بمرحلتين :
وتعمل نقطة الوصول بمهمات عديدة منها التنسيق وتسجيل المحطات والتحقق من هوياتهم ويتم التعرف على نقطة الوصول عن طريق عنوانها الفيزيائي .

١- -ترسل المحطة لاولى الاطار لنقطة الوصول

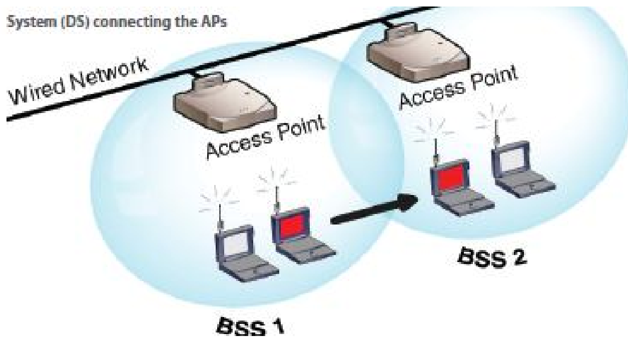
٢- ترسل نقطة الوصول الاطار الى المحطة الهدف

في كل الاتصالات التي تجري عبر نقطة الوصول تكون منطقة الخدمة الرئيسية متطابقة مع نمط BSS والمعرف بواسطة النقاط والتي يمكن لها الاتصال مع نقطة الوصول أي في مجال عملها .
وعلى الرغم من ان الارسال المتعدد أو البث يحتاج لسعة اكبر من الاطار المرسل الى المستقبل مباشرة

- يعرف النمط BSS بالمسافة اعتبارا من نقطة الوصول . وكل المحطات المتنقلة mobile stations تحتاج لان تكون في منطقة عمل نقطة الوصول ولكن لاتحديد لاماكن توضع المحطات بالنسبة

لبعضها وان السماح بالاتصال المباشر بين المحطات سيوفر سعة الارسال ولكن تكلفة زيادة تعقيد الوسط الفيزيائي ستكون كبيرة .بما انه يجب على المحطات ان تصون علاقات الجوار مع كل المحطات في منطقة الخدمة .[14][17]

يشير مصطلح Extended Service Set (ESS) الى مجموعة مكونة من اثنين او اكثر من BSS وتشكل مايسمى single sub-network وبما ان معظم الشبكات اللاسلكية للشركات تحتاج الى الاتصال بالشبكة السلكية من اجل الخدمات (المخدمات – الطابعات– نقاط الاتصال بالانترنت ..) لذلك سوف تعمل في نمط البنية التحتية



الشكل (١-٦) يبين نمط العمل ESS [14]

٢- نموذج الشبكة المتكافئة AD HOC

تعود تسمية هذا النموذج كونه يتم بشكل مرتجل دون تخطيط وهو مناسب للحالات الطارئة مثل غرف المؤتمرات وتعمل محطات العمل كمجموعة خدمة مستقلة IBSS) Independent Basic Service Set) دون الاعتماد على نقطة الوصول وتتواصل المحطات اللاسلكية ضمن مجال البث المحدود الشكل (١-٧) .



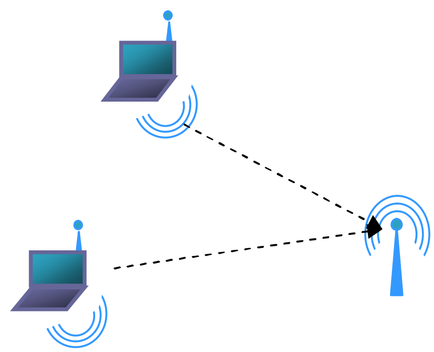
الشكا (١-٧) يبين نمط الند AD HOC [1]

١-٣ طريقة عمل الشبكة الحاسوبية اللاسلكية

يتم تهيئة نقاط الوصول من قبل مدير الشبكة ويسند لكل نقطة رمز تعريف SSID ويمكن أن يتم الاتصال بين الزبون ونقطة الوصول بطريقتين الطريقة الأولى تعتمد على إرسال نقطة الوصول إطار مرشد لاسلكي يتضمن إضافة لمعرف نقطة الوصول عنوانها الفيزيائي والطريقة الثانية تعتمد على اخفاء المعرف وذلك حسب إعدادات الشبكة واهنا نميز :

١-٣-١ المسح الخامل: (السبر الفعال) **Passive Scanning**

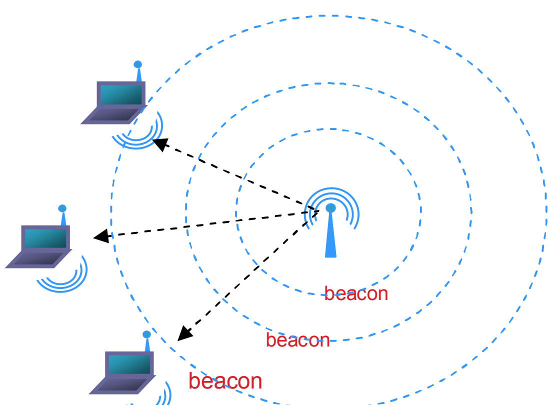
ترسل محطة الزبون إطار طلب سبر Probe Request وتجيب نقاط الوصول بإطار استجابة Probe Response وعندئذ تختار المحطة نقطة الوصول المطلوبة للاتصال معها او إتمام الإجراءات [5]



الشكل (١ -٨) يبين طريقة السبر الفعال

١-٣-٢ : المسح الفعال **Active Scanning**

تقوم محطة الزبون بمسح المجال الراديوي لمعرفة الشبكات الفعالة لجميع القنوات والاستماع لها بهدف كشف مرشد المحطة وهذا مبين في الشكل (١-٩) ، ولهذه الطريقة سيئة مهمة تتلخص في عدم قدرتها على اكتشاف الشبكات اللاسلكية المعدة لعدم ارسال المعرف ESSID أو الطريقة المخفية اضافة الى ذلك هذه الطريقة تتطلب ان يتصل الزبون مع نقطة الوصول بشكل فعال وهو مايعطي مراقب الشبكة فرصة لمعرفة المحطات غير الموثوقة .



الشكل(١-٩) يبين طريقة المسح الفعال

١-٣-٣- المراقبة الراديوية **RF Monitoring**

ان التطبيقات التي تستخدم تقنية RFMON تستطيع مقاطعة واظهار المعلومات عن الشبكات التي تلتقطها , وسوف تقوم بذلك بدون تحديد وجود فقط المعلومات المكتشفة في إطارطلب السبر واجابته .

كما في التقنية الكامنة فمن الصعب للمحلل الدخيل ان يكتشف هذا النشاط في طبقة MAC ان تقنية المسح الخامل السبر الفعال لاتعطي للمهاجم فرصة كبيرة لمحاولة اقتحام الشبكة .

لاتستطيع الزبائن اللاسلكية في حالة RFMON ارسال أي اطارات ولكن فقط تستطيع الاستقبال ولهذا السبب فهي تلتقط الاطارات وان الزبون الذي يستخدم المراقبة الكامنة Passive Monitoring يستطيع ان يقدم تقريره عن عناوين الـMAC ومرافقاتها لنقطة الوصول المكتشفة ، ولكن لايستطيع ان يسبر نقطة الوصول من اجل ارسال معلومات عن طريق بروتوكول SNMPويتسطيع ان يرسل تقريراً عن نتائج طلب GET في SNMP و اذا كان الطلب بدا من كرت شبكة مختلف من زبون على نفس التردد وفي نفس زمن المهاجم .

ان برمجيات الاكتشاف تقاطع هذه المعلومات وترسلها الى المهاجم وعندها يتمكن المحلل الدخيل من مراقبة تدفق المعلومات في الشبكة في الطبقة الثالثة بالادوات المعروفة باحثا عن اشارات السبر معتمدا عل المعلومات المزيفة (على سبيل المثال مراقبة اوامر SNMP الخاصة بجمع معلومات غير صحيحة) .

١-٤ بنية الإطارات اللاسلكية

يعرف المعيار ٨٠٢,١١ ثلاث فئات من الإطارات MAC وهي:

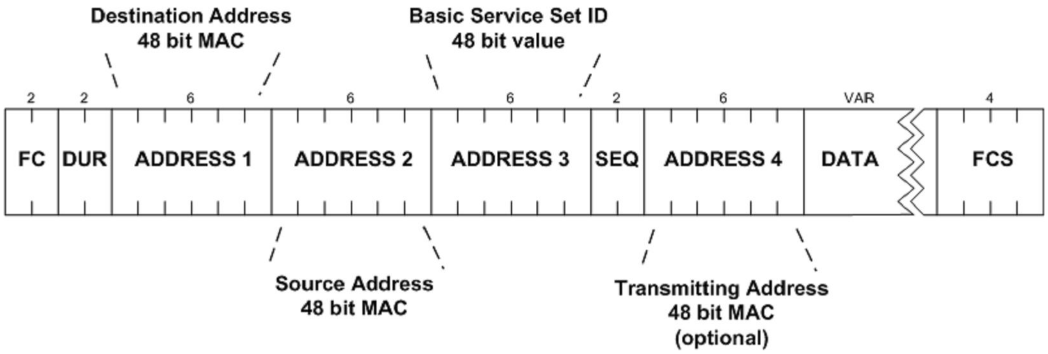
- إطار بيانات ، بسيطة أو مزودة ببعض الخصائص .
- إطار تحكم ، ويمكن أن يشير إلى توفير الطاقة أو الإقرار ...
- إطار إدارة ، مثل طلب الإنضمام ، أو إطار المرشد اللاسلكي ، أو المصادقة وغيره .

ولكل منها هامش ً يتضمن حقولاً متنوعة مستعملة ضمن الطبقة MAC وهناك بعض الهوامش المستعملة من الطبقة الفيزيائية وهي على الغالب متعلقة بتقنيات التعديل المستعملة [15][13] .

حيث يخصص اطار المعيار 802.11 بايتين لحقل التحكم المتسلسل sequence control fields بحيث يخصص ٤ بتات لحقل التجزئة و ١٢بت للرقم المتسلسل sequence number وعندما تطلب اطارات المعلومات أو اطارات الادارة ان تتجز أ يتم الارسال في اجزاء ويتم زيادة ارقام التجزئة fragment numbers لكل جزء أو باكيت وتقوم محطة الاستقبال باعادة تجميع التدفق برقم تسلسل ثابت constant sequence number في حقل التحكم control field .

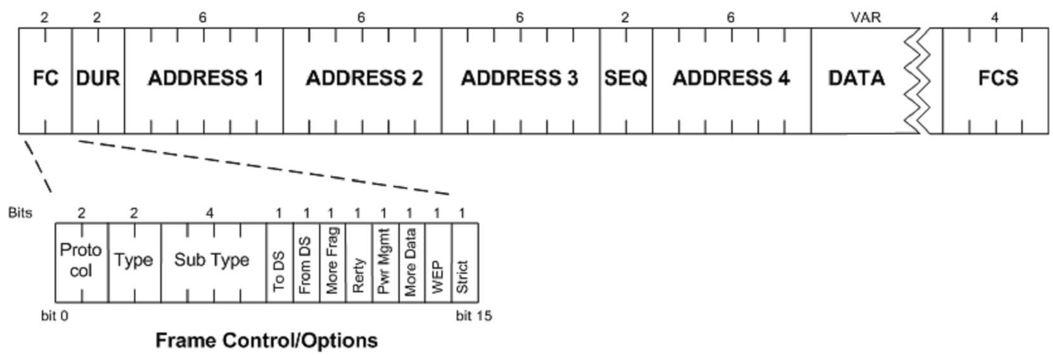
ان رقم تسلسل الحقل هو عداد تسلسلي ويزيد في كل اطار غير مجز أ ويبدأ بالرقم صفر وهو من الدارات 4096 ان رقم التجزئة هو دائما صفر حتى يتم تجزئة الباكيت الكبير

يبن الشكل التالي الإطار القياسي للمعيار 802.11



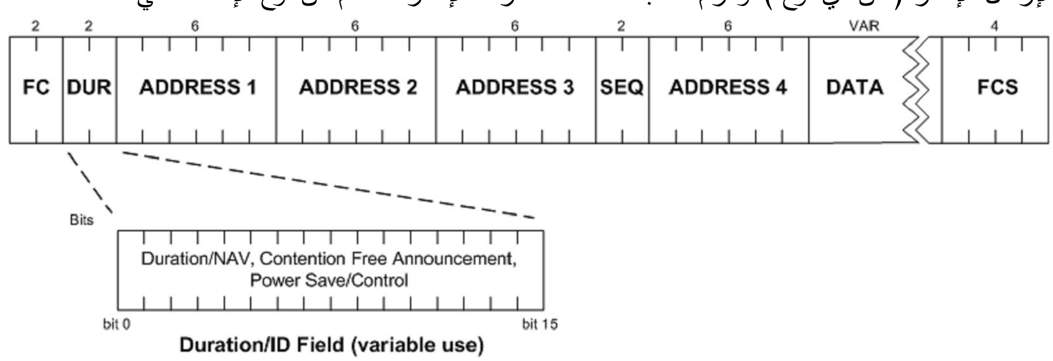
الشكل (١-١٠) يبن اطار المعيار 802.11 [9]

■ **الحقل الأول حقل التحكم بالاطار frame control FC هو** وهو مبين بالشكل (١-١١) وهو مؤلف من أحد عشر حقلاً فرعياً تتعلق بنسخة البروتوكول ومحتوى الإطارات والنوع الفرعي للإطار وحقل إدارة الطاقة وحقل الخوارزمية وغيرها.



الشكل (١-١١) يبن بنية حقل التحكم في اطار المعيار 802.11 [9]

■ **الحقل الثاني الدور DUR** مبين في الشكل (١-١٢) وهو بطول ٦ ابت مزدو ج الوظيفة فهو يبين الزمن اللازم لإرسال الإطار (من أي نوع) أو رقم مطابقة المحطة المرسلة لإطار التحكم من نوع الإقتصاد في الطاقة .



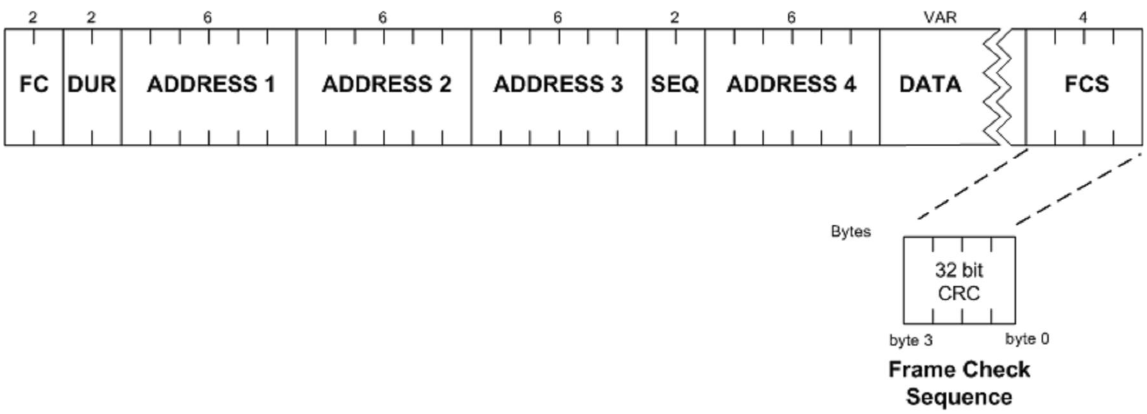
الشكل (١-١٢) يبين حقل الدور في اطار المعيار 802.11

■ **حقول العناوين Address1,2,3,4** وهي أربعة جميعها حسب مقياس 802 وكل حقل يتألف من ٦ بايت أو 48 bit تشكل عنواناً ثابتاً للمستقبل أما القسم الثالث فهو ٦ بايت تشكل العنوان الفيزيائي للمرسل أما القسم الرابع فهو مؤلف من العنوان الفيزيائي لمحطة العمل أو نقطة الوصول BSSID .

■ **حقل التحكم المتتالي SEQ** مؤلف من حقلين الأول رقم التجزئة Fragment Number بطول 4bit وهو يبين عدد الأجزاء للرزمة MSDU نظير في الطبقات الأعلى من طبقة وصل المعطيات بنفس الرقم ولايستطيع أي مهاجم تغيير هذا الرقم الفريد .

والثاني هو رقم التسلسل المرجعي Sequence reference number بطول 12bit يبين الرقم المرجعي للرزمة MSDU المسند إليه اثناء إرسال المحطة حمولتها .

■ **الحقل FCS الحقل الأخير** هو حقل التحقق من الرقم التسلسلي فهو حقل تحقق مؤلف من ٣٢بت الهدف من التأكد من الرقم التسلسل للإطار وضمان عدم تغييره وهو يعمل بطريقة CRC.



الشكل (١-١٣) يبين حقل التحقق من الرقم التسلسلي في اطار المعيار 802.11

١-٥ تحليل عمل الاطارات اللاسلكية وفق المعيار ٨٠٢,١١

بعد تحليل مجموعة من الشبكات اللاسلكية العاملة وفق المعيار 802.11 وجدنا عدة حقول من الإطار يجب الاهتمام بها وتحليلها لدراسة امن الشبكة الحاسوبية اللاسلكية ومن هذه الحقول :

١- حقل الرقم التسلسلي : **Sequence number Field**

ان حقل التحكم المتسلسل كما ذكرنا سابقا يستخدم ليميز التجزئة في شبكات المعيار 802.11 ، في حال ظهور نفس رقم sequence number فهذا يشير الى حدوث سرقة للجلسة sniffer .

٢- حقل ضبط النوع أو النوع الجزئي **Control Type and Subtype**

يستخدم هذا الحقل 2byte من اطار التحكم وفق معيار 802.11 لتعريف المعطيات ، تستخدم اطارات التحكم والادارة لدعم نمط الارسال لشبكات 802.11 وهي بشكل عام تحوي 00/0100 (ارسال اشارة الطلب Probe

Request) و 00/0101 (استجابة اشارة الطلب (probe response) و 00/1000 لاشارة beacon و 10/0000 للمعلومات .

٣- العنوان الفيزيائي لنقطة الوصول AP MAC Adrress :

ان الزبون الذي يبحث لاكتشاف الشبكات اللاسلكية المتاحة عبر المسح الفعال يرسل اطار طلب الى طبقة MAC من نقطة الوصول متمثلاً بالعنوان .("FF:FF:FF:FF:FF") وهو عنوان بث ، عندئذ ينتظر جواباً متضمناً العنوان الفيزيائي لنقطة الوصول .

٤- معرف الخدمات (Service Set Identifier (SSID

بالاضافة لاعداد عنوان MAC يتم ضبط معرف الخدمات على القيمة "0x00" في اطار الطلب، ان آخر محطة تتصل في IBSS مسؤولة عن الاستجابة لطلب اشارة PROBE واذا كانت الشبكة من نوع BSS تحوي AP فانه يستجيب للاشارة .

٥- المعرف المميز للمنظمة (Organizationally Unique Identifier (OUI

وهو جزء من تغليف اطار 802.2 وهو يتالف من ٣ بايتات تستخدم لتمييز المصنع كجزء من التوضيح لتعريف بروتوكول الادارة المحلي . وهذه القيمة سوف توضع بشكل شائع على ٠ لكل اطارات اثرنت المغلفة .

٦- حمل المعلومات Data Payload

يمكن ان يحتوي هذا الحقل في اطارات LLC معلومات فريدة في تعريف برنامج الاستكشاف الذي يولد التدفق .

٧- حقل نوع بروتوكول LLC LLC Protocol Type Field

يحدد هذا الحقل نوع بروتوكول الطبقة العليا وكمثال 0x0800 لتدفق IP و 0x0806 لـ ARP 0x888e لمصادقة 802.1x 802.1x authentication.

٨- رقم تعريف بروتوكول LLC LLC Protocol ID

وهو جزء من ترويسية SNAP ، يستخدم هذا الرقم لتحديد نوع البروتوكول المستخدم وخاصة في المعرف المميز للمنظمة OUI المحدد في الاطار.[5] .

١-٦ بروتوكولات نقل البيانات Data Transfer Protocol

تضم هذه المجموعة من البروتوكولات كل من البروتوكولين TCP و UDP وتستخدم هذه البروتوكولات في إطار بحثنا لاختبار إنتاجية Throghput الشبكة المحلية اللاسلكية وذلك عند تطبيق بارامترات أمنية عليها مثل بروتوكولات الأمن المختلفة .

١-٦-١ بروتوكول التحكّم بالنقل Transmission Control Protocol (TCP)

بروتوكول التحكّم بالنقل Transmission Control Protocol (TCP) هو بروتوكول لنقل المعلومات مبني على إقامة الإتصال Connection-Oriented يوفّر النقل الموثوق للبيانات بين عمليتين Processes. يضمن هذا البروتوكول وثوقية نقل البيانات عبر تطبيق آليّات التحكّم بتدفق البيانات Flow Control وتصحيح الأخطاء Error Correction.[13]

يتم التحكّم بسيل البيانات بين المرسل والمستقبل باستخدام النوافذ متغيرة الحجم Sliding Windows، قواعد تغيير حجم النافذة Window Size Adjustment Heuristics وخوارزميّات تجنّب الإزدحام Congestion Avoidance Algorithms تضمن هذه الآليّات الثلاث التوزيع العادل لموارد الناقل المشترك على جميع جلسات الإتصال Sessions الفعّالة.

تتألّف آليّة تصحيح (أو التحكّم) الخطأ في بروتوكول TCP من رسائل تأكيد الإستلام Acknowledgement المرسلة لكل حزمة تم استلامها بنجاح، كما تتحكّم هذه الآليّة بإعادة إرسال حزم البيانات في حين لم يتم استلامها بشكلٍ صحيح. يلائم بروتوكول TCP التطبيقات التي تحتاج إلى نقل البيانات بشكلٍ موثوق (مثل HTTP، FTP، SMTP وغيرها).

١-٦-٢ بروتوكول رزمة المستعمل User Data Protocol (UDP)

يوفّر بروتوكول رزمة المستعمل User Data Protocol (UDP) (وهو أحد بروتوكولات طبقة النقل Transport Layer) خدمة نقل البيانات بالجهد الأقصى Best Effort لا يمكن الوثوق بهذه الخدمة لأنّها لا توفّر الحماية من النسخ المتعددة لحزم البيانات أو ضياع هذه الحزم. لا يحتوي بروتوكول UDP على أيّة آليّاتٍ للتحكّم بسيل البيانات أو تصحيح الأخطاء. يعتبر المجموع الخاص لحمل البيانات Checksum الأسلوب الوحيد المستخدم في بروتوكول UDP للتحقق من سلامة البيانات المنقولة. يقوم المستقبل لدى اكتشافه حزمة بياناتٍ تالفةٍ بإهمال هذه الحزمة دون أن يحاول أن يطلب من المرسل إعادة إرسالها.

يلائم بروتوكول UDP تطبيقات الزمن الحقيقي Real Time Applications (RTA) حيث تعتبر سرعة نقل البيانات أكثر أهميّةً من وثوقية خدمة النقل.

الخصائص	UDP	TCP
جودة الخدمة QoS	الجهد الأقصى، غير موثوقة	خدمة موثوقة
الوصلة	لا يعتمد على إقامة الإتصال Connection-less	يعتمد على إقامة الإتصال Connection-Oriented

تأكيد الإستلام	غير موجود	يتم تأكيد إستلام جميع البيانات
إعادة الإرسال	غير موجود	م إعادة إرسال البيانات المفقودة تلقائيّاً
اتحكّم بسيل البيانات	غير موجود	النوافذ متغيرة الحجم Sliding Windows، تعديل حجم النافذة، تجنّب الإزدحام
الحمل الإضافي	خفض جدّاً	نخفض لكنّه أكبر من بروتوكول UDP
سرعة الإرسال	رتفعة جدّاً	رتفعة لكنّها أقل من بروتوكول UDP
ملائم لـ:	١. عندما تكون سرعة نقل البيانات أكثر أولويةً من الوثوقيّة ٢. نقل حزم البيانات الصغيرة ٣. عند استخدام البث Broadcast أو الإرسال لعدة أطراف Multicast	ﺎلبيّة البروتوكولات

جدول (٢–١) مقارنة بين خصائص بروتوكولي TCP و UDP [19]

المعيار	**نوع التعديل**	**معدل تدفق البيانات الأعظمي عبر الوصلة (Mbps)**	**معدل تدفق البروتوكول TCP (Mbps)**	**معدل تدفق البروتوكول UDP (Mbps)**
802.11b	CCK	11	5.9MBPS	7.1
802.11b/g	OFDM/CCK	54	14.4	١٩,٥
802.11g	OFDM/CCK	54	٢٤,٤	٣٠,٥
٨٠٢,١١n	OFDM/MIMO	٧٢	٣٦	٤٢
٨٠٢,١١n	OFDM/MIMO	٣٠٠	١٤٤	١٧٧

جدول (٣–١) يبين مقارنة بين معدلات تدفق المعلومات في معايير الشبكات اللاسلكية المختلفة [14]

الفصل الثاني

نظام أمن الشبكات الحاسوبية اللاسلكية
WLAN Security System

مقدمة : يتم بناء نظام أمن الشبكات WLAN بواسطة مجموعة متنوعة من البروتوكولات تتضمن هذه البروتوكولات خوارزميات التشفير وترميزات كشف الأخطاءو غيرها كما يهدف نظام أمن الشبكة اللاسلكية إلى تحقيق مجموعة من الأهداف والمعروفة بخدمات الأمن [13]، منها :

١. **خدمة السرية Confidentiality** : لتأمين حماية بيانات المستخدم عن طريق أنظمة اتشفير المختلفة
٢. **المصادقة Authentication** : تهدف لتأمين موثوقية الاتصال أو الرسالة بين طرفين وعدم تدخل طرف ثالث ضمن عملية الإتصال .
٣. **تكاملية البيانات Integrity** : هذه الخدمة تعمل على منع تغيير أو تعديل البيانات إلا من قبل الأشخاص المخولين بذلك .
٤. **التوفر Availability** : تؤمن هذه الخدمة ، الوصول الموثوق إلى المعلومات عند الحاجة إليها
٥. **عدم الإنكار Non –repudiation** تضمن هذه الخدمة ، لمستقبل الرسالة البرهان على هوية المرسل وعدم نكران المرسل أو المستقبل للإتصال أو محتوى الرسالة .

٢-١ بروتوكولات أمن الشبكات اللاسلكية Wireless Security Protocols

عرفت الشبكات WLAN مجموعة من البروتوكولات التي تحمي الوصول للشبكات اللاسلكية وتشفر البيانات وفق خوارزميات محددة منها :

٢-١-١ بروتوكول السرية المكافئة Wireless Equivalent Privacy (WEP)

صمم البروتوكول بهدف تامين مستوى امني مماثل للمستوى الامني في الشبكة اللاسلكية وهو يعمل بمستوى طبقة وصل البيانات وهو آليه حماية بسيطة للبيانات المرسلة من محطة الزبون الى نقطة النفاذ ويعد البروتوكول WEP نظام تشفيرمتناظر ، اذ يستعمل نفس المفتاح في قسمي التشفير وفك التشفير ، لكن المعيار 802.11 لم يبين طريقة توزيع المفتاح علما ان هذه العملية تحتاج لبروتوكول ادارة مفاتيح

اعتمد البروتوكول WEP في البداية على مفتاح تشفير بطول 40bit وهو المفتاح السري للنظام وتم استبداله لاحقا بمفتاح bit ١٠٤ و BIT ١٢٤ يشكل هذا المفتاح مع شعاع الاقلاع مفتاحا اطولا لتطبيقه على مداخل خوارزمية

التشفير RC4 [21] [13] يعتمد البروتوكول WEP على نظام RC4 وهو نظام تشفير مستمر ومتناظر ويدعم مفاتيح بطول متغير لتوليد سيل المفاتيح الضرورية لعملية التشفير

يعاني البروتوكول WEP من مجموعة من نقاط الضعف وأهمها :

١- استعمال مفاتيح WEPساكنة ومشتركة بين الز بائن لفترة طويلة وعدم وجود ادارة للمفاتيح

٢- محدودية فراغ شعاع الاقلاع بحجم ٢٤ بت وارساله بشكل صريح أو إعادة استعماله

٣- ان شعاع الاقلاع بحجم ٢٤بت هو جزء معروف من مفتاح خوارزمية التشفير RC4

4- عدم وجود آليه كريبتوغرافيه لحماية تكاملية البيانات إذ يستعمل الترميز الدوري .

Mac Header	IV	Zero Reserved	Key ID	Data	ICV	FCS
32 octets	3 octets	6 bits	2 bits	0-2312 bits	4 octets	4 octets

In the clear Encrypted In the clear

الشكل (٢-١) يبين إطار بروتوكول WEP [14]

يمكن استعراض بعض الوسائل لتقوية النظام الأمني المبني على WEP وهي :

- زيادة حجم شعاع الاقلاع
- بعثرة القيمة IV والحاقها بالنص المشفر بدلا من شكلها الصريح
- استعمال وسائل التحقق من البيانات بديلة عن الترميز الدوري، مثل توابع البعثرة
- تبديل المفتاح السري باستمرار وباستعمال بروتوكولات توزيع متناظرة آمنه
- اعتماد بروتوكولات المصافحة الآمنة لادارة توزيع المفاتيح

2-1-2 بروتوكول المفتاح المؤقت Temporal Key Integrity Protocol (TKIP)

تم اقتراح البروتوكول لتجاوز ثغرات البروتوكول WEP اضافة الى تأمين التوافقية الخلفية مع WEP بحيث تنفي الحاجة الى استبدال الكيان المادي الداعم للبروتوكول WEP .

يمثل البروتوكول TKIP سلسلة من أربع خوارزميات مصممة لتقوية البروتوكول WEP وهي

١- MIC (Message Integrity Chek)

٢- Extended 48-Bbit IV & IV Sequencing

٣- Per Packet Key Mixing

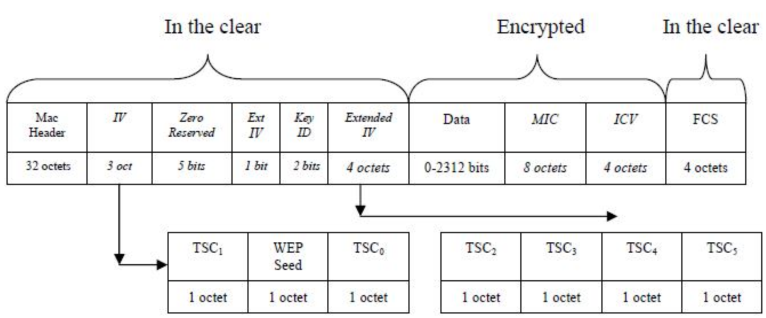
٤- Rekeying

تصبح الخوارزميات الأربعة متاحة لدى اعداد نقطة النفاذ ويمكن تنشيط TKIP كوحدة ولكن ليس في جميع نقاط النفاذ بل بحسب المصنع .

يعمل البروتوكول TKIP على تجاوز ضعف خوارزمية الترميز الدوري المستعملة مع البروتوكول WEP باستعمال الخوارزمية MIC لضبط صحة البيانات عن طريق البعثرة اللاخطية لمنع تعديل البيانات وهي تنفذ فعليا بواسطة خوارزمية ميكائل Michael لانخفاض اعباء الحسابات لهذه الخوارزمية .

كذلك يعمل البروتوكول TKIP لمنع اعادة استعمال قيمة شعاع الاقلاع عن طريق اضافة العداد TKIP Sequence Counter (TSC) بحجم ٤٨ بت بحيث يضمن شعاع اقلاع وحيد لكل باكيت (بالتالي مفتاح مختلف لكل باكيت مما يقلل من احتمالات تخمين المفتاح) [14][8]

بالمقارنة مع WEP يعتبر البروتوكول TKIP مكلفا وربمايخفض أداء نقطة الوصول وهذا البروتوكول يستخدم خوارزمية RC4 للتشفير ولكن يتخلص من نقطة ضعف المفتاح ويجبر على توليد مفتاح كل ١٠٠٠٠ باكيت بالاضافة لذلك يبعثر Hashes شعاع الاقلاع والتي ترسل كنص صريح في WEP .



الشكل (٢-٢) يبين إطار بروتوكول TKIP [14]

٢-١-٣ بروتوكول الوصول المحمي Wi-Fi Protected Access (WPA) :

دفعت مظاهر الضعف في البروتوكول WEP بتحالف الشركات WI-FI الى اقتراح نظام النفاذ المحمي Wi-Fi Protected Access (WPA) وقد صمم ليعمل بنمطين :

١- النمط الشخصي **Personal** : ويسمى نمط المصادقة البسيط pre –shared key وهو لايتطلب مخدم مصادقة ويكتفي بالمصادقة مع نقطة النفاذ باستعمال المفتاح المشترك .

٢- **نمط الشركات أو المؤسساتي Enterprise** : يتطلب مخدم مصادقة مبني بواسطة البروتوكول RADIUS للمصادقة وتوزيع المفاتيح مع ادارة مركزية لاعتماد الزبائن مع المعيار 802.1X يوزع مفاتيح مختلفة لكل مستخدم .

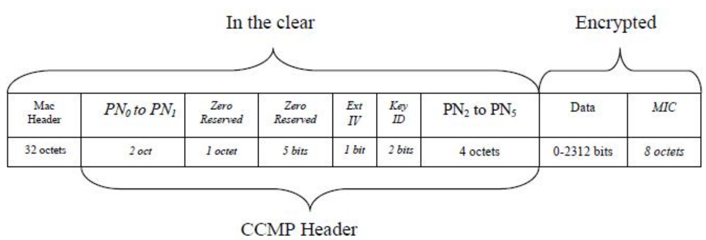
يعد البروتوكول WPA جزءاً من المعيار 802.11i وقد تجاوز هذا البروتوكول مظاهر الضعف التي عاناها بروتوكول WEP والمتمثلة في استخدام مفاتيح ضعيفة ومحدودية فراغ شعاع الاقلاع مماسمح لادوات المخترقين من تخمين المفتاح من خلال تحليل التدفق اللاسلكي .[13][8]

٢-١-٣-١ كسر البروتوكول WPA-PSK WPA-PSK Cracking

ان الهجوم المعروف بـ Brute-force أو البحث الشامل والذي يوجد العديد من البرمجيات المنفذه له يستطيع كسر البروتوكول WPA-PSK بواسطة اختبار العديد من كلمات السر المختلفة وتركيبة المحارف ويستطيع برنامج مثل WPAtty اختبار ٧٠ كلمة بالثانية بواسطة جهاز بسرعة معالج 3.8Ghz [5] .

٢-١-٤ بروتوكول CCMP :

تعود تسمية البروتوكول CCMP الى العبارة CTR With CBC-MAC Ppotocol ويعد هذا البروتوكول مركزياً بالنسبة للشبكات المتماسكة أمنيا RSN وفقا للمعيار 802.11i تم بناء البروتوكول CCMP باستعمال خوارزمية التشفير المعيارية AES ذات المفتاح المتناظر والتي تدعم علباً بحجم ١٢٨بت ومفاتيح تشفير بحجوم مختلفة لكن البروتوكول يستعمل مفتاحا بحجم ١٢٨ بت وهي تؤمن أعلى درجات الأمن في المرحلة الحالية .
يؤمن البروتوكول CCMP حماية اطار البيانات ومعظم الهامش MAC من خلال خوارزمية MIC منعا لاستغلال الهامش من قبل المهاجم يُستعمل رقم خاص للباكيت PN لمنع هجوم الاعادة Replay attacks ، ويتطلب البروتوكول CCMP مفتاحا جديدا لكل جلسة ويتم تأمين ذلك من مميزات خوارزمية التشفير AES .



الشكل (٢-٣) يبين إطار بروتوكول CCMP [14]

٢-١-٥ بروتوكول الوصول المحمي Wi-Fi Protected Access 2 (WPA2)

اطلقت هذه النسخة من البروتوكول في ايلول ٢٠٠٤ وان المعيار 802.11i [20]عنون ثلاثة أهداف رئيسية لهذا البروتوكول وهي :

- المصادقة
- ادارة المفاتيح

- وحماية خصوصية تدفق المعلومات

اعتمد معيار التشفير المتقدم Advanced Encryption Standard (AES) وهو متوافق مع البروتول الأقدم WPA ويمكن ان يعمل بنمطين، الشخصي والمؤسساتي ويمكن أن يعمل بنمط مختلط WPA/WPA2 mixed mode ولايعمل WPA2 مع بعض انواع بطاقات الشبكة القديمة
ان خوارزمية التشفير المستخدمة في المعيار 802.11i تعمل بالنمط التشغيلي AES-Counter Mode CBC-MAC Protocol (AES-CCMP) وتستخدم بلوك التشفير AES ولكنها تقيد طول المفتاح الى ١٢٨ بت ، وتستخدم تقنيتي .(counter mode and CBCMAC)
ان تقنية العداد تستخدم رقماً عشوائياً يتغير مع كل بلوك من النص وهذا يجعل من الصعب جدا كسر هذا التشفير

أما بروتوكول CBC-MAC protocol (Cipher Block Chaining- Message Authentication Code) فهو يستخدم للتحقق من سلامة الرسالة والتأكد من ان بتات النص الصريح لم تتغير .[16]
يبين الجدول التالي مقارنة بين طرق التشفير السالفة الذكر :

مقارنة بين طرق التشفير للشبكات الحاسوبية WLAN			
اسم البروتوكول	WEP	WPA(TKIP)	WPA2 (CCMP)
خوارزمية التشفير	RC4	RC4	AES
طول المفتاح (بت)	١٠٤/٤٠	١٢٨	١٢٨
حجم شعاع الاقلاعIV (بت)	٢٤	٤٨	٤٨
تكاملية البيانات	CRC-32	Michael Algorithm	CCM
ادارة المفاتيح	None	EAP BASED	EAP BASED
المستوى الأمني	ضعيف	متوسط	عالي

الجدول (٢-١) يبين مقارنة بين طرق التشفير للشبكات الحاسوبية WLAN [13]

ومما سبق يمكن أن نعرف سويتين من الخوارزميات الأمنية وبالتالي المستويات الأمنية وهي :

① خوارزميات لبناء شبكة بمستوى أمني بسيط Pre –RSN Algorithm والتي تتضمن

- خوارزمية WEP

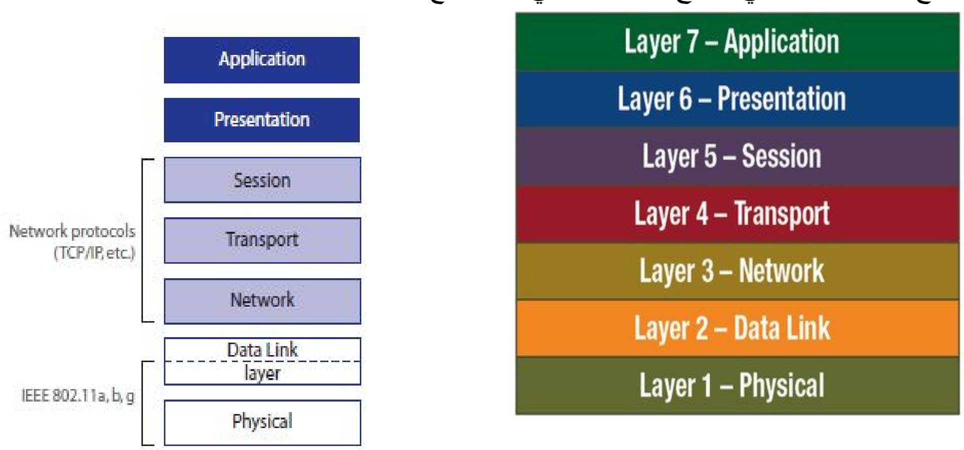
- بروتوكولات المصادقة البسيطة IEEE 802.11

② خوارزميات لبناء شبكة متماسكة أمنياً RSN Algorithm والتي تتضمن :

- بروتوكول TKIP
- بروتوكول CCMP
- بروتوكولات تأسيس وا ٍنهاء RSN بما فيها استخدام IEEE 802.11
- بروتوكولات إدارة المفاتيح **Conclusion**

٢-٢ الأمن عبر طبقات الشبكة

بشكل نظري يمكن أن تتم الحماية في أي طبقة من الطبقات السبع للنموذج OSI المبين في الشكل (١-٥) ولكن بشكل عملي فان أمن الشبكة مرتبط بأمن الاطارات في الطبقة الثانية وأمن الباكيتات في الطبقة الثالثة . الشكل (٢-٤) يوضح طبقات الشبكة في نموذج OSI المرجعي مقارنة مع طبقات الشبكة الحاسوبية اللاسلكية



الشكل (٢-٤) يظهر طبقات الشبكة حسب نموذج OSI [7]

٢-٢-١-أمن الطبقتين الثانية والثالثة : المزايا ونقاط الضعف

بما ان تقنيات التشفير متمركزة في الطبقتين الثانية والثالة ومع انتشار الانترنت تستطيع معظم اجهزة التشفير في الاسواق ان تعمل في الطبقة الثالثة حيث يستخدم بروتوكول IPSec

ومع انتشار الشبكات وازدياد التدفق في التطبيقات الكثيرة كالصوت والفديو والوسائط المتعددة الاخرى تظهر محدودية عمل هذا البروتوكول وخاصة فيما يتعلق بالمردود في حال استخدامه ويصبح غير عملي .

اما معالجة الأمن في الطبقة الثانية فإنه يجعل العملية بسيطة وخارج تعقيدات جداول التوجيه والتي تضيف عبئاً غير ضروري على العملية ،ويصبح التدفق معزولاً ومحمياً في الوسط اللاسلكي ، بواسطة انشاء " قنوات " عبر الشبكة العاملة .

وبالاضافة الى ذلك تنشئ الطبقة الثانية اتصالاً فيزيائياً بين الزبائن والنقاط البعيدة وتعرف اطار المعلومات في وسط الاتصال بين العقد . تستخدم اتصالات الطبقة الثانية اوليا لنقل البيانات عالية السرعة ، وتغلف آليات التشفير كل بروتوكولات الطبقة العليا عبر الوصلة .

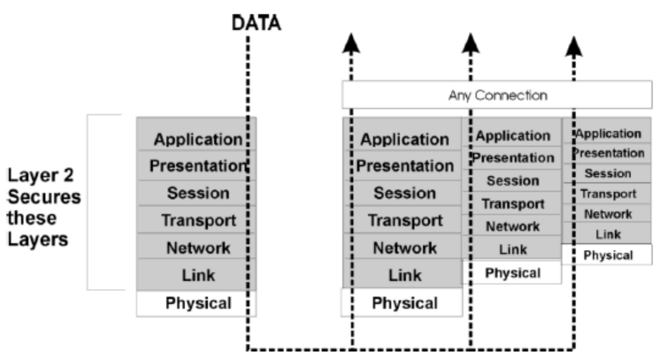
بشكل مثالي ينجز تشفير الطبقة الثانية في معظمه عندما يكون الوسط مشفراً بالكامل أو بنظام القنوات عندما يشفر حمل المعلوماتdata payload فقط في اطار اثرنت .

تشفر التطبيقات اللاسلكية من نقطة لنقطة ، ان التطبيقات المستخدمة في شبكات التبديل تستعمل الاقنية النفقية Tunneling لتبقى معلومات ترويسة الاطارغير مشفرة وتشفير باقي الحمل .

٢-٢-٢ الامن في طبقة وصل البيانات مع بروتوكول WPA :

تقدم طبقة وصل البيانات الامن من نقطة لنقطة بين اجهزة شبكية متصلة مباشرة ويتضمن ذلك ارسال اطارات امنه مبرمجة تحتوي مصادقة دخول المستخدم User authentication وتشفير الاطار Frame encryption والتحقق من تكاملية البيانات المرسلة Data integrity verification

وهذا يعني ان امن هذه الطبقة يقدمها كطبقة امنة للخارج وان حماية طبقة وصل البيانات تبدا بخدمة المصادقة Authentication service وتتضمن خدمتي التشفير و سلامة البيانات



الشكل (٢-٥) يبين الطبقات التي تقوم طبقة وصل البياناتبتأمين الحماية لها

تتميز طبقة وصل البيانات والتي هي الاكثر عرضة للهجوم بالخصائص التالية :

١- بصمة صغيرة والتي تمكنها من التكامل مع بطاقات ملائمة الشبكة ونقاط الوصول Access Point واجهزة الموبايل و آليات هذه الطبقة تتكامل معظم الاحيان مع التجهيزات Hardware .

٢-تسمح لبروتوكولات الطبقات العليا مثل IP وIPX ان تمر بأمان وهذا يعني تقديم الامان لكافة بروتوكولات الطبقات العليا

ان مصطلح WI-FI قد اخذ يستعمل بواسطة IEEE 802.11TGi بتقنية المفاتيح الموزعة لانتاج معيار جديد هو Wi-Fi Protected Access (WPA). وهو معيار صناعي لتزويد الشبكاتاللاسلكية بامن شبكة قوي جداً على مستوى طبقة وصل البيانات ،وتزويدها ببروتوكولين لادارة المفاتيح هما Extensible Authentication Protocol (EAP وبروتوكول TKIP اضافة الى بروتوكول التحقق من تكاملية الرسالة Message Integrity Check (MIC) [3]

٢-2-٣ حماية WLAN بالترابط مع تشفير الطبقة الثانية

كما هو معروف ان التقنيات اللاسلكية هي الحل في البيئات التي تكون فيها الحلول السلكية مكلفة وغير عملية ، ولكن ارسال المعلومات الحساسة عبر الهواء أمر محفوف بالمخاطر ويطرح تحياً لنظام الأمن من الهجمات النشطة والساكنة ويعتبر تشفير الطبقة الثانية العامل الأساسي في حماية الشبكة اللاسلكية من التهديدات المفترضة [7] . إن المقصود بوسط الإرسال هو الوصل اللاسلكي وتحت هذه المظلة ينضوي عدد كبير من تقنيات الوصل التي تستخدم مثل المجال الراديوي Radio frequency ،ومجال الأمواج الميكروية Microwave , ، مجال الفراغ الحر الضوئي .Free-space optics .

تعاني طرق الوصل اللاسلكية من ثغرات هامة في مجال الامن ، وكما هو في أي وسط مفتوح إن تاكيد الوثوقية والصحة للبيانات الحساسة المنقولة عبر هذه الشبكات أمر في غاية الصعوبة وخاصة في التطبيقات الحكومية والعسكرية . ان التحديات الأمنية موجودة في المعلومات المرسلة والتي تتضمن الهجمات الفعالة والساكنة .

ان الهجوم الساكن يحدث عندما يقوم المهاجم بجمع وقراءة المعلومات الحساسة المرسلة ، في حين يحدث الهجوم الفعال عندما يقوم المهاجم بحقن تدفق جديد في الشبكة عندما يخرق أمنها .وهذا مايدفعنا لدراسة هذه التهديدات ومعرفة كيفية حدوث الخروقات وخاصة في الطبقتين المسؤولتين الثانية والثالثة .

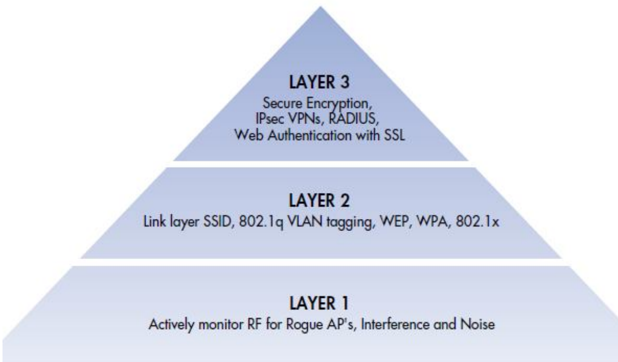
٢-٢-٤ تكامل حماية الشبكات اللاسلكية

لقد تم تصميم بروتوكول التشفير WPA خصيصا للشبكات اللاسلكية وهو يزود المستخدمين بحماية للمعلومات ويسمح فقط للمستخدمين المخولين بالوصول للشبكة وهو ليس فقط زيادة عن حماية بروتوكول WEP القديم بل هو يزود بحماية فعالة من الهجومات غير الهادفه مثل DOS او الهادفة مثل Peer to Peer Attack وهو يعمل مع معظم تجهيزات الشبكة ويقدم مايلي :

١- يحسن كل ثغرات الخصوصية في WEP
٢- يحسن بشكل دراماتيكي امن WI-FI
٣- متطلب اساسي في معايير WI-FI Q3 2003
٤- لم تخترق النسخة الثانية منه حتى الان بهجوم معروف
٥- يتطلب مخدم مصادقة Authentication server
٦- يستخدم بروتوكولات RADIUS للمصادقة وتوزيع المفاتيح
٧- مناسب للاستخدامات المتنوعة منزلية, اعمال صغيرة , والاعمال الكبيرة

٢-٢-٥ مقارنة بين الأمن في طبقتي وصل البيانات والشبكة :

يمكن اعتبار امن الشبكة اللاسلكية مؤلفا من اجتماع امن الطبقين الثانية والثالثة وبإدراك امن كل طبقة يستطيع مدير الشبكة ان ينشئ نظام حماية فعالاً باعتبار ان أمن طبقة الشبكة يتم عبر بروتوكول IPSec وباستخدام القنوات المحمية VPN والتي تؤمن حماية للتدفق بين المستخدم وتجهيزات محددة ولاتحمي من الاخطار الاخرى على المجال الراديوي المشترك ان كلفة الحماية في الطبقة الثالثة باهظة مقارنة مع الحماية في الطبقة الثانية التي تتم عبر بروتوكولات التشفير المستخدمة .كما يجب على مديري الشبكة تحسين أمن الشبكة في الطبقة الثانية باستخدام EAP وهكذا نجد ان الحماية الكاملة للشبكة تكون بتضافر جهود الحماية في الطبقتين الثانية الثالثة و مع بعضها البعض . [4]

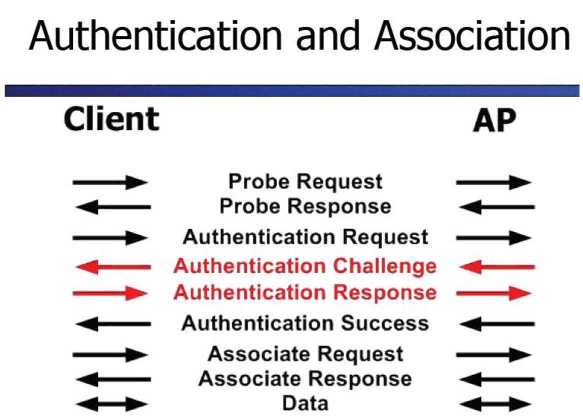


الشكل (٢-٦) يبين الحماية في الطبقات الثلاثة [5]

٢-٣ المصادقة والترابط في شبكات WLAN

تعتبر عمليتي المصادقة والترابط في الشبكات الحاسوبية اللاسلكية خطوتين أساستين لكل زبون لاسلكي يحاول الدخول للمجال اللاسلكي وتجري العمليتين بشكل متتالٍ مع أن عملية المصادقة هي الخطوة الأولى والأساسية

وستتركز دراستناعلى متطلبات هذه العملية وطرقها وأنواعها [14] :



الشكل (٢-٧) يوضح عمليتي المصادقة والترابط بين الزبون ونقطة الوصول

2-3-١ عملية المصادقة Authentication Process

تتم عملية المصادقة في الشبكات المحلية اللاسلكية بمرحلتين :

١- طور المصادقة

٢- طور التشفير

في المرحلة الاولى يطلب الزبون اللاسلكي الاتصال بنقطة الوصول معلنا عن نفسه وعن العنوان الفيزيائي لكرت الشبكة الخاص به وهنا وبحسب معيار 802.11 الاساسي يمكن أن تتم عملية المصادقة اما بالنمط المفتوح Open authentication أو بنمط بروتوكول السرية المكافئ WEP أو بروتوكولات الوصول المحمي بإصداراتها المختلفة .

تتضمن عملية المصادقة تبادل مجموعة من الرسائل

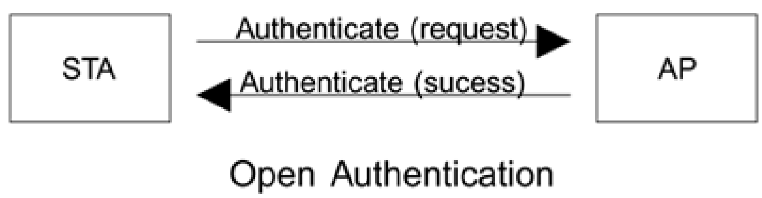
وتقسم الرسائل المتبادلة الى ثلاثة انواع :

١- رسائل تحكم

٢- رسائل ادارة

٣- معلومات

المصادقة المفتوحة تتم عبر رسالتين' الأولى ، من الزبون بطلب الوصول ' والثانية من نقطة الوصول بنجاح العملية[12] كما هو مبين في الشكل (٢-٨):

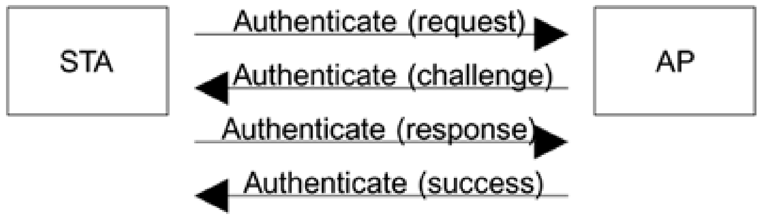


الشكل (٢-٨) يبين عملية المصادقة المفتوح [22]و[23]

واحيانا تتم المصادقة المفتوحة باستخدام تشفير WEP الذي يستخدم لتشفير البيانات بالمفتاح المشترك بعد عملية المصادقة ولايشفر عملية المصادقة [14]

اما المصادقة باستخدام بروتوكول WEB فهو يشمل أربع مراحل وهي :

يرسل الزبون اللاسلكي طلب الاتصال تستجيب نقطة الوصول بارسال نص للزبون لتشفيره يسمى challenge message باستخدام المفتاح المشترك secret key يرسل الزبون اللاسلكي النص المشفر واذا كان صحيحا ترسل نقطة الوصول رسالة نجاح المصادقة كما هو في الشكل التالي



WEP Authentication

الشكل (٢- ٩) يبين عملية المصادقة باستخدام بروتوكول WEB [22]و[23]

٢-٣-٢ بنية اطارات المصادقة :

تتالف بنية جميع اطارات المصادقة من الاقسام التالية

Algorithm Num	Transaction Seq.	Status Code	Challenge Text

- الحقل The Algorithm Number يشير الى نوع المصادقة المستخدم

0 ? Open system
1 ? Shared key (WEP)

- الحقل The Transaction Sequence يشير الى تتالي عمليات المصادقة

- الحقل The Status Code يشير في نهاية الرسالة الاخيرة الى نجاح او فشل عملية المصادقة

The Challenge Text يستخدم في حالة المصادقة باستخدام WEP لتشفير النص بالمفتاح المشترك [22]

٢-٤ تحسين أمن الشبكات الحاسوبية اللاسلكية

يمكن تحسين نظام أمن الشبكات WLAN بواسطة مجموعة من الطرق والأساليب منها :

٢-٤-١-لائحة التحكم بالوصول Acess Control Lists ACLs

يستخدم العنوان الفيزيائي MAC ضمن طبقة وصل البياناتكآلي ّة ٍ لتحديد وعنونة مصدر البيانات المرسلة إلى مضيف ٍ معي ّن ٍ مرتبطٍ بقناة ٍ مشترك. يتألّف هذا العنوان من تسلسل ٍ فريد ٍ يحتوي على ٨ بايت ّاً (١٢ رقماً ست عشري ّاً) مرتبطٍ ببطاقة ٍ شبكة ٍ لاسلكية ٍ أو منفذ الجهاز الشبكي يكون العنوان الفيزيائي عادة ً مثبّ ّتاً ضمن التجهيزات عندما يقوم المنتج بشحنها كما تقوم بطاقة الشبكة عادة ً بتمرير رزم البيانات التي توافق العنوان الفيزيائي للحاسب فقط إلى نظام التشغيل.[22]

تحتوي ترويسحزم البيانات المرسلة عبر ناقلٍ مشتركٍ عناوين حواسب المصدر والوجهة لهذه البيانات. يتم استخدام عنوانٍ خاصٍ عند إرسال رزم إلى جميع الحواسب بطريقة البث يدعى عنوان البث وهو يعادل في شبكات الإيثرنت العنوان ff:ff:ff:ff:ff:ff(جميع البتّات الـ ٤٨ تساوي ١).

تعتبر لائحة التحكم بالوصول ابسط طرق الامن لشبكة الحواسب اللاسلكية وان الحماية المقدمة بهذه الطريقة تتم عن طريق فلترة جميع طلبات الاتصال الواردة الى نقطة الوصول عبر برمجة العنوان الفيزيائي للأجهزة المخولة بالدخول الى الشبكة في نقطة الوصول وحينها فقط للزبائن المخولين authorized client's تستطيع الاتصال مع نقطة الوصول واي اتصال اخر يرفض .

ان هذه الطريقة تقدم حماية للشبكة خلف نقطة الوصول ولاتحمي الزبون اللاسلكي ولا سلامة التدفق الشبكي وهذا مايجعل هذه الطريقة عرضة للاختراق لانه يمكن اختطاف جلسة لزبون مخول واعادة ارسالها لنقطة الوصول أو تحليل الاتصالات لمعرفة العنوان الفيزيائي المتاح وبرمجة هذا العنوان في كرت شبكة لاسلكي آخر وهذه العملية تسمى انتحال العنوان MAC spoofing [11]

وهذه العملية متاحة بشكل بسيط في نظام التشغيل لينوكس عبر هذه التعليمات :

```
ifconfig eth0 hw ether 00:01:02:03:04:05
Where:
eth0 is the network interface we want to modify.
00:01:02:03:04:05
```

ان البحث داخل نقطة الوصول عن العنوان الفيزيائي للتأكد من وجوده يتم بطريقة تتابعية لايجاد القاعدة المناسبة وتنظم لوائح التحكم بالوصول لاخذ هذا العامل بعين الاعتبار بسبب الزيادة المضطردة في متطلبات الامن وتصنيف الباكيتات فان الزمن اللازم لذلك اصبح يشكل قدرا مهما في عملية المصادقة Aathentication اضافة الى ان هذا الزمن متغير ويضيف تأخيرا على عملية تحويل الباكيتات من خلال نقطة الوصول ويؤدي الى عبء اضافي لوحدة المعالجة داخل نقطة الوصول وخاصة في حالة العدد الكبير من العناوين الفيزيائية المطلوب برمجتها . [16] [10]

تقوم بعض مخدمات المصادقة RADIUS باستلام طلب من نقطة الوصول يحتوي معرف مستخدم USER ID والذي يربطه مع العنوان الفيزيائي لهذا المستخدم ويمكن ان يخزن هذه العناوين لديه بدلا من ذاكرة نقطة الوصول . [20] ومن المفيد قياس زمن المصادقة ومراقبة تأثير تفعيل لائحة التحكم بالوصول على زمن المصادقة وزمن كسر الشيفرة والبارامترات الأخرى وتم تحقيق ذلك من خلال البحث .

٢-٤-٢ بروتوكول التوزيع الآلي لعناوين الشبكة (DHCP) Dynamic Host Control Protocol)

يعمل هذا البروتوكول على مخدم شبكة محلية مخصص لهذا الغرض ، ويتيح المضيف الحصول على عنوان الانترنت بشكل آلي وديناميكي مجرد انضمامه للشبكة ويدعم هذا البروتوكول انضمام الاجهزة المتنقلة اللاسلكية مثل الحواسب المحمولة

كذلك يعمل DHCP على تزويد اطار لتمرير معلومات الهيكلة الى المضيف في شبكة TCP/IP ويعدهذا البروتوكول امتدادا للبروتوكول BOOTP (Bootstrap Protocol) الذي يعمل على استنهاض المضيفين البعيدين عبر الشبكة ، ويضيف بروتوكول DHCP امكانات التخصيص الالي لعناوين الشبكة المعاد استخدامها مع خيارات الهيكلة الاضافية .

يعتمد بروتوكول DHCP في عمله على تبادل مجموعة من الرسائل وفق بروتوكول UDP المنفذ 67 بين الزبون والمخدم وهذه الرسائل مبينة في الجدول (٢-٢) :

DHCP DISCOVER	رسالة تبث من الزبون بهدف ايجاد مخدم DHCP
DHCP OFFER	رسالة جواب من المخدم تعرض عنوان IP وبارامترات اخرى
DHCP REQUEST	رسالة من الزبون الى المخدم ولها الاحتمالات التالية : • يطلب البارامترات المعروضة من احدى المخدمات ويرفض العروض الاخرى • يطابق العنوان المخصص سابقا بعد التغييرات التي حصلت في الشبكة • يطلب تمديد الاجار لعنوان محدد
DHCP ACK	رسالة اقرار من المخدم الى الزبون بالبارامترات بما فيها IP ADDRESS
DHCP NACK	رسالة اقرار سلبية من المخدم الى الزبون تبين أن استئجار الزبون قد نفذ أو أن طلب العنوان IP غير صحيح
DHCP DECLINE	رسالة من الزبون الى المخدم تبين ان العنوان المقدم هو قيد الاستعمال
DHCP RELEASE	رسالة من الزبون الى المخدم يلغى فيها ماتبقى من الاستئجار وهو يتخلى عن عنوان الشبكة
DHCP INFORM	رسالة من الزبون والذي حصل مؤخرا على عنوان IP يطلب بارامترات الهيكلة الاخرى من المخدم DHCP

الجدول (٢-٢) يبين انواع رسائل DHCP [13]

يتكون البروتوكول DHCP من مركبتين:

■ البروتوكول الذي يحرر بارامترات الهيكلة الخاصة بالمضيف من المخدم

■ آلية لتخصيص عناوين الشبكة المؤقتة أو الدائمة الى المضيف

يدعم بروتوكول DHCP ثلاث آليات لتخصيص العناوين IP

١- التخصيص الالي للعنوان حيث يسند البروتوكول عنوانا دائما للمضيف

٢- التخصيص الديناميكي اذ يتم تخصيص عنوانٍ لفترة محددة من الزمن (يدعى عنوانا مستأجرا) وهي الالية الوحيدة التي تسمح باعادة استعمال العناوين آلياً .

٣- التخصيص اليدوي اذ يتم تخصيص العنوان من قبل مدير الشبكة .

وهناك بروتوكول خاص بين المضيف والمخدم لطلب العنوان يتلخص بالخطوات التالية :

■ يبث المضيف رسالة DHCP DISCOVER للبحث عن المخدم .

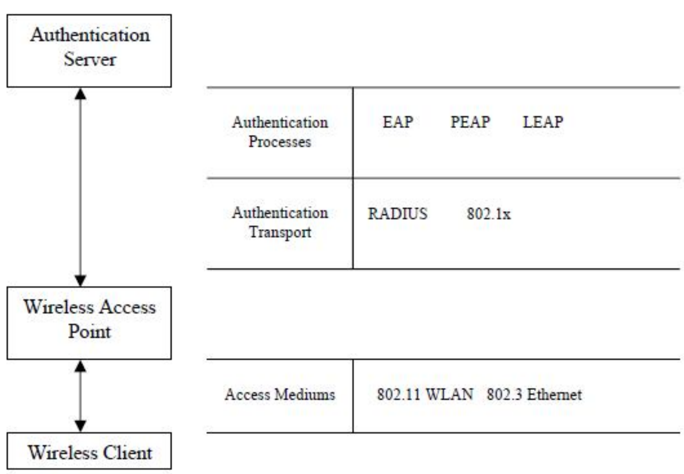
■ يجيب المخدم برسالة DHCP OFFER عرض تخصيص عنوان

■ يطلب المضيف عنوان IP عبر رسالة DHCP REQUEST

■ يرسل المخدم DHCP عنوانا عبر رسالة اقرار DHCP ACK

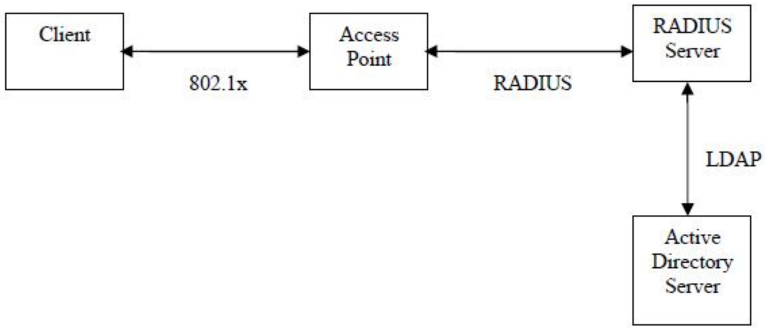
٢-٤-٣ استخدام RADIUS SERVER لتحسين امن الشبكة اللاسلكية

تم اشتقاق التسمية من Remote Authentication Dial In User Service و هو مخدم مخصص لأغراض المصادقة مع ادارة للمفاتيح وهو يعمل وفق المعيار 802.1X وهذا المعيار يصف بروتوكول من طبقة وصل البيانات يستعمل لنقل بروتوكولات مصادقة من المستويات الأعلى [14][15][16]



الشكل (٢-١٠) يبين عملية المصادقة باستخدام مخدم توثيق [14]

يعد المعيار 802.1X طريقة للتحكم بالوصول الى الشبكة عن طريق المنافذ وهو ينفذ عند ارتباط الزبون بالشبكة وهو يعمل بين برنامج الزبون المسمى Supplicant وجهة المصادقة مثل نقطة الوصول وهنا لابد من وجود طرف ثالث لاتمام عمليات المصادقة وهو المخدم والذي يكون عادة مبنياً بواسطة البروتوكول RADIUS

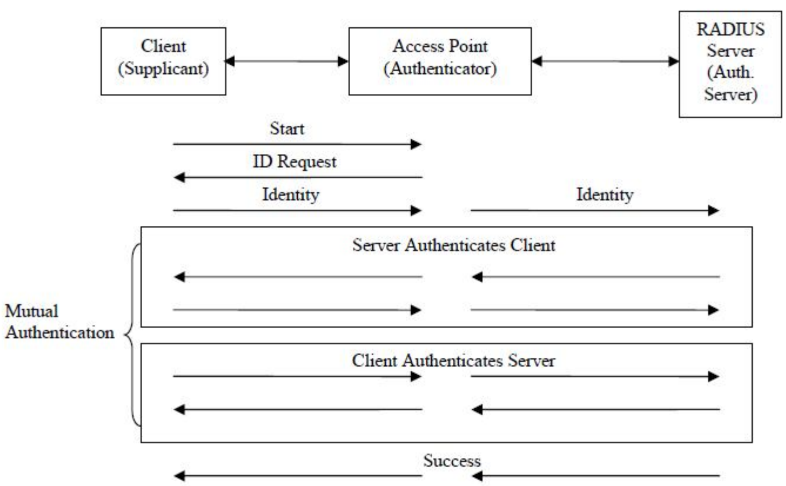


الشكل (٢-١١) يبين احدى تشكيلات مخدم RADIUS [14]

٢-٤-٣-١ بروتوكول المصادقة الموسع (EAP) Extensible Authentication Protocol

يعمل البروتوكول على نقل معلومات المصادقة بشكل حمل(EAP) ويتوضع جهاز المصادقة في الوسط لينقل حمل EAP على شكل باكيتات 802.1X الى المخدم وفق البروتوكول RADIUS المخصص للاتصال بين جهاز الشبكة ومخدم المصادقة ويسمح بنقل ازواج من القيم مثل معلومات الدخول الى الشبكة USERNAME /PASSWORD [16]

ويعمل EAP بالطريقة المبينة في الشكل التالي :



الشكل (١٢-٢) يبين المصادقة بواسطة EAP

يتيح البروتوكول عدة طرق للمصادقة أهمها :

EAP-MD5

يتم بعثرة اسم المستخدم وكلمة السر بواسطة الخوارزمية ويعاني الضعف بسبب هجوم Man-In- Middle Attack

EAP-TLS

يدعم هذا البروتوكول عدة ميزات منها المصادقة المتبادل وتبادل المفاتيح وتتابع الجلسات والتي تزيد من أمن النظام وهو يحتاج لسبع خطوات لاتمامه

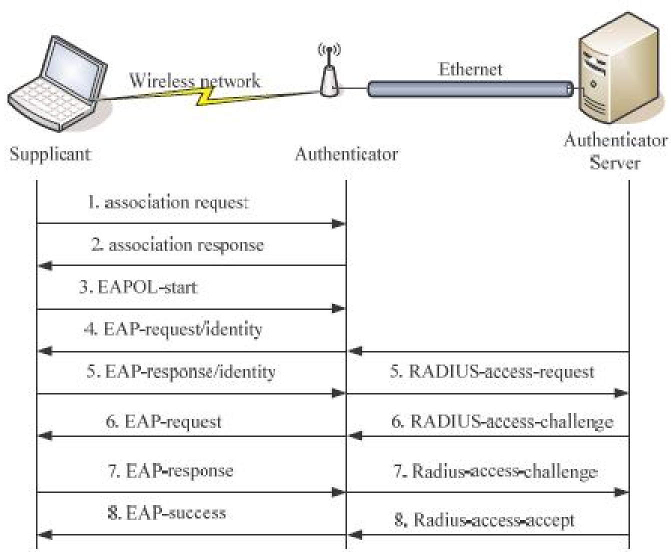
EAP-TLS supports

يدعم المصادقة المتبادل وتبادل المفاتيح والتقسيم والتجميع واعادة الاتصال لان هذا البروتوكول يدعم الجلسات المتتابعة وهذا مايسرع عملية اعادة المصادقة [14][1]

يعاني هذا البروتوكول من هجوم MAN-IN Middle Attack الذي يستطيع اختراق الجلسة [16]

٢-٤-٣-٢ بروتوكول (Extensible Authentication Protocol On LAN (EAPOL

يستخدم البروتوكول EAPOL لإرسال المعلومات بين الزبون ونقطة الوصول (جهاز المصادقة) بينما يستخدم البروتوكولان EAP , RADIUS لارسال الباكيتات بين المصادق ومخدم المصادقة RADIUS SERVER كما في الشكل (٢-١٣) [15]



الشكل (٢-١٣) رسائل EAPOL المتبادلة عبر 802.1x [15]

❋ ❋ ❋ ❋ ❋ ❋ ❋

الفصل الثالث

الهجمات والتهديدات في الشبكات الحاسوبية اللاسلكية
WLAN, Attacks and Threats

مقدمة : إن اعتماد الشبكات WLAN على البث اللاسلكي بأجواء مفتوحة خلق لهذه الأنظمة تحديات خطيرة متمثلة بإمكانية الوصول الى منطقة البث لاسلكيا مما يتيح اختراقا غير محسوب العواقب ويمكن أن يشكل تهديدا جديا لنظام الشبكة مما يحد من استخداماتها في الاماكن التي تحتاج لسرية المعلومات اضافة الى محدودية السرية هناك المدى والسرعة والفاعلية .

و انطلاقا من مكونات الشبكة WLAN الأساسية (– **نقاط الوصول** – **محطات الزبائن** – **وسط الإرسال الراديوي**) ، يمكن استشراف أنواع التهديدات التي يمكن أن تتعرض لها الشبكات اللاسلكية بما يلي :

١– نقاط الوصول غير المرخصة Unauthorized access points

٢– بث مجموعات تعريف الشبكة Broadcasted SSIDs,

٣– المحطات المجهولة Unknown stations

٤– العناوين القفيزيائية الـ MAC المزيفة Spoofed MAC addresse

٣–١ : ادوات وطرق الاختراقات Hackers Tools and Methods

إن هدف المخترق هو كسر امن الشبكة لذلك يلجا للبرمجيات التي تطور خصيصا لكسر التشفير حيث يقوم بتجريب البرمجيات وتقنيات الدخول لمسح الشبكة المستهدفه ومعرفة نقاط الضعف وأهم الادوات المستخدمة لاختراق الشبكة هي :[6]

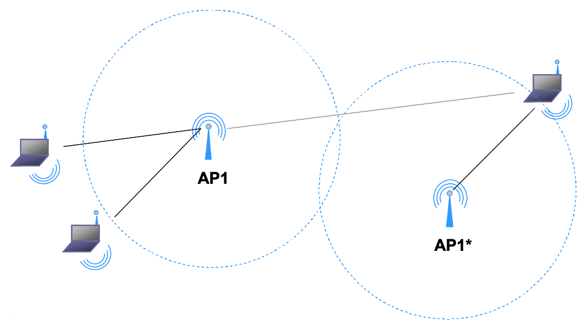
١. الهوائيات **Antennas**: وتستخدم لاكتشاف اشارة الشبكة اللاسلكية وفق معيار 802.11

٢. ادوات كسر الشيفرة برمجيا **Encryption breaking tools** : مثل برنامج airsnort ,wep cracker والتي تحاول ان تجلب المعلومات المرتدة والتي ستستخدم لاحقا في كسر مفاتيح التشفير .

٣. التجسس عن طريق القيادة **War Driving**: وهنا يستخدم المهاجم اجهزة المسح scanner واجهزة السبر probing devices مثل برنامج Netstumbler لاكتشاف الشبكات ونقاط الوصول التي تستخدم لبرمجة الشبكة وكذلك قنوات البث ويرسل المهاجم معلومات وخرائط الى الشبكة العالمية عن الشبكات التي تم اختراقها. وربما يحتاج الى هوائيات تقوية لزيادة مدى الشبكة التي يلتقط اشاراتها عن بعد

٤. الترابط الخادع **Malicious Association** :

يمكن ان يتم هذا الترابط باستخدام ادوات تسمى toll HostAP والتي تمكن جهاز الاختراق من تحويل نقطة الوصول التي يتصل بها المستخدمون الى نقطة وصول افتراضية انشأها المخترق [6] وهذا مبين في الشكل (٣-١)



الشكل (٣-١) يبين طريقة الترابط الخادع

٣-٢ تصنيف الهجمات في الشبكات الحاسوبية اللاسلكية WLAN :

٣-٢-١ هجوم منع الخدمة **Denial of Service Attack (DOS)**

الهدف من هذا الهجوم احتكار الموارد في الشبكة وحجبها عن المستخدمين وهذا النوع من الهجوم يمنع المستخدمين المخولين من الوصول للموارد التي يطلبونها وفي الشبكات التي تعتمد IPSec يجب في هذه الحالة تحويل التدفق عبر الشبكة السلكية وهذا سيسمح للمستخدمين الشرعيين لاقامة اتصال عبر IPSec ولكنه سيسمح لمستخدمين متنوعين لارسال اطارات والتي يمكن ان تقبل من نقطة الوصول وان يصل المهاجم الى المعلومات مقاطعا للمستخدمين المخولين وربما يحصل ذلك عندما يحصل المهاجم على رسالة ملتقطة من اتصال ما ويعيد ارسالها لنقطة الوصول .

٣-٢-٢ هجوم الرجل في الوسط **Man-in-the-Middle Attack** .

ان طبقة الشبكة لاتقدم حماية الا لبروتوكول IP تاركة البروتوكولات الاخرى معرضة للهجوم احد الهجمات التي يمكن أن تتم عبر بروتوكول ARP Address Resolution Protocol المتمثل بتبديل العناوين IP الى عناوين فيزيائية MAC وهكذا ينتحل عنوان IP من جلسة حيث تتم معالجتها من قبل نقطة الوصول وتبديل عنوان فيزيائي لزبون مخول عبر بروتوكول ARP .

٣-٢-٣ هجوم الند للند Peer-to-Peer Attack .

غالبا مايستخدم IP SEC لضمان امن الاتصال بين المستخدم ونقاط الوصول وبدون امن لطبقة وصل البيانات سوف تقوم نقطة الوصول بجلب بيانات لمستخدمين مخولين وغير مخولين وهنا يمكن للمستخدمين غير المخولين من مراقبة تدفق المعلومات والتقاط المعلوما مثل IP شبكة مجاورة ومن ثم الهجوم على هذه البطاقة التي تحمل هذا الرقم .

٣-٢-٤ هجمات حقن الشبكة Network injection

في هذا النوع من الهجمات بامكان المهاجم ان يستخدم نقطة وصول معرضة لتدفق شبكة غير مفلتر وخاصة تدفق البث حيث يقوم المهاجم بحقن أوامر تهيئة التي تغير مواصفات الموجه أو الموزع وفي هذه الحالة فان كل الشبكة تصبح خارج الخدمة وتحتاج الى اقلاع جديد أو تهيئة جديدة [[3].

٣-٢-٥ هجوم Caffe Latte :

يخصص هذا الهجوم لمعرفة كلمة السر في البروتوكول WEP حيث يستهدف امن نظام التشغيل
حيث يرسل سيلاً من طلبات ARP المشفرة ويقوم باستقبال الاجابة ويستخدم مفتاح الشبكة بعدها لتوثيق دخوله بشكل صريح .[3]

٣-٢-٦ هجوم البحث الشامل Brute force attack :

وهو هجوم منظم يختبر عدة أحرف , ارقام ورموز حتى يخمن كلمة السر.وهناك عدد كبير من البرمجيات المتاحة على الانترنت لهذا الغرض مثل .AirSnort [4] and WEPCrack [5]
ويحتاج برنامج AirSnort لالتقاط حوالي ٥-١٠ مليون رزمة مشفرة وحالما يتم الجمع يتم فك الشيفرة وخاصة في WEP لان شعاع الإقلاع Initialisation Vector يرسل بنص غير مشفر ضمن الرزم المشفرة وهذا يعني ان أي ملتقط للمعلومات بشكل متلصص Sniffer package وان البروتوكول الجديد WPA يمكن اختراقه باستخدام هجوم Dictionary brute-force attack والذي يستطيع اختبار ٧٠ كلمة سر / في الثانية بمعالج سرعتهGHZ ٣,٨[8]

٣-٢-٧ هجوم ARP :

يستخدم هذا الهجوم لمتحويل عناوين IP الى عناوين MAC في قطاع الشبكة المحلية والتي يملك فيها المضيفون HOSTS نفس القناع . ان هجوم ARP يحدث عندما يحاول احدهم تغيير جداول ARP ل MAC و IP بدون تخويل . وعندها باستطاعة المخترقين انتحال هذه العناوين والقيام بهجومين معروفين، ايقاف الخدمة والرجل في الوسط .[17]

٣-٢-٨ هجوم سرقة الجلسة Session High Jacking :

وهو هجوم موجه لسلامة الجلسة حيث يقوم المهاجم بسرقة جلسة مخولة وموثقة من صاحبها المفترض ، الذي يعرف بانه لم يعد يمتلك الجلسة ولكن لايعرف بسرقتها بل ربما يعتقد بفقدانها بسبب خطا في الشبكة اللاسلكية . وحالما يحصل المهاجم على جلسة صالحة يقوم بزيادة زمنها وهذا يحدث بالزمن الحقيقي ولكن يستطيع العمل بعد اعتقاد ضحيته ان الجلسة انتهت .

٣-٢-٩ هجوم الإعادة Replay :

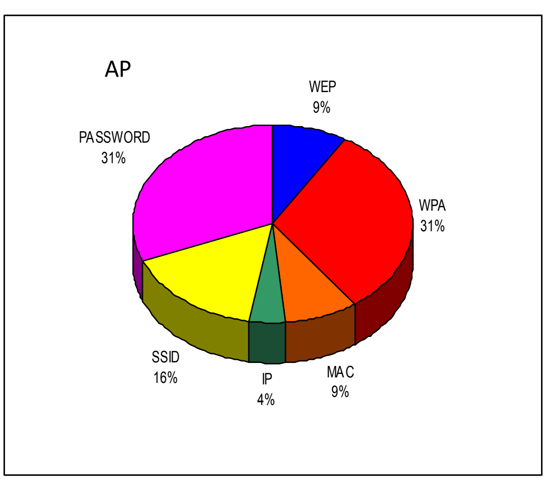
وايضا هذا الهجوم يخص سلامة المعلومات في الشبكة اذا لم يكن هناك ضرورة لسلامة جلسة محددة ويستخدم هذا الهجوم للحصول على وصول للشبكة بتخويل من الهدف ، ولكن الجلسات الحقيقية لم تتاثر بهذا الجمع وهذا الهجوم ليس بالزمن الحقيقي حيث يستطيع الوصول للشبكة في بعض الاوقات بعد انتهاء الجلسات الاصلية . يقوم المهاجم في هجوم الاعادة بالتقاط تخويل الجلسات ثم يعيد التخويل في وقت لاحق أو يجمع عدة جلسات ليركب التخويل ومن ثم يفتح التخويل بدون مفتاح [8]

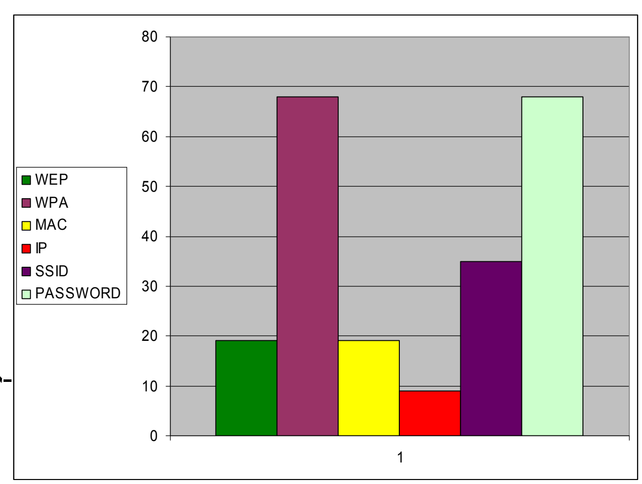
٣-٢-١٠ اكثر الطرق الأمن استخداما في الشبكات اللاسلكية :

يوضخ الشكل (٣-2) طرق الامن الاكثر شيوعا في الشبكات اللاسلكية وخاصة انه يمكن الجمع بين اكثر من طريقة واحدة مثل الفلترة والتشفير والطرق المتاحة للأمن هي [7] :

- **تشفير WEP**
- **تشفير WPA (TKIP,CCMP)**
- **فلترة عناوين MAC**
- **اخفاء معرفات الشبكة SSID**
- **تغيير كلمات مرور الموجه PASSWORDS**

يمكن توزيع طرق الحماية المستخدمة بالشكل التالي كنسبة مئوية :





الشكل (٣-2) يبين أهم طرق الأمن المتبعة [7] الشكل (٣-3) توزيع بارامترات الأمن كنسبة مئوية

وهذا مايبرر تركيزنا في هذا البحث على بارامترات الأمن مثل بروتوكولات الأمنWEPو WPA1 و WPA2

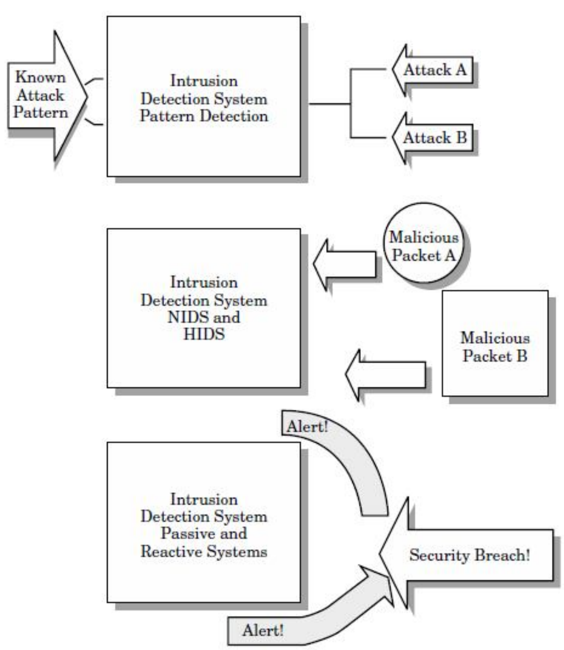
وكذلك استخدام لوائح التحكم بابوصول ACL و مخدمات المصادقة Radius Servers .

٣-٣ نظام كشف الاختراق في الشبكات IDS/ WLAN:

ان اختلاف نظام عمل الشبكة اللاسلكية عن الشبكة السلكية التقليدية يجعل من الصعوبة على النظام اكتشاف الاختراقات وخاصة ان الشبكة اللاسلكية تعتمد على البث اللاسلكي مما يتيح لمتطفلين غير معروفين في الشبكة من التقاط البث ومحاولة الاقتحام عن بعد مما يجعل من المحتم على النظام معالجة كم هائل من الاطارات والرزم غير معلومة المصدر والتي يجب ان تعالج قبل وصولها الهدف ويطلق على عملية المعالجة هذه بتقنية التخطيط العكسي Reverse mapping للتحقق من مصدر هذه الرزم أو الاطارات قبل وصولها الى نظام التتبع والتحليل .ان تعرض الاشارة اللاسلكية للضياع يطرح مشكلة في وصول هذه الرزم الى IDS [4]

٣-٣-١ بينة نظام كشف الإختراق IDS

يقوم نظام ids والذي يعتمد على التعرف الالي على الهجمات والمخترقين بفحص وتحليل كل الفعاليات الداخلية والخارجية والنوع الأولي من ids موضح بالشكل (٣-٤) [10] :



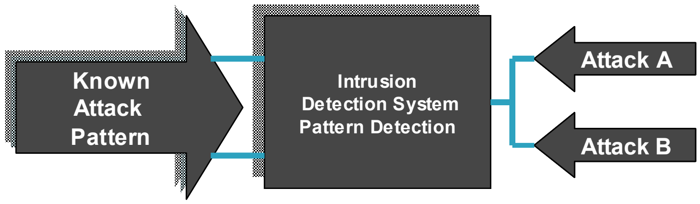
الشكل (٣-٤) يوضح بنية IDS [16]

٣-١-١-١ كشف النموذج Pattern detection :

يقوم IDSبتحليل المعلومات التي جمعها ويقار نها مع التواقيع المميزة للهجومات الموجودة في قاعدة بياناته ويبحث في هذه القاعدة عن نموذج الهجوم الذي سجله الآن لتحديد طبيعته وهذه النمط البرمجي مناسب فقط في حال وجود تواقيع هذا الهجوم معروفه ومخزنه مسبقا .

كما يستطيع مدير النظام ان يراقب الفعاليات التي تمر بشبكته مثل ازدحام الشبكة و نقاط الخلل والبروتوكولات المستخدمة وحجم الرزمة النظامي كما يراقب اجزاء الشبكة ويقارن ذلك مع الحالة الطبيعية ويحدد نماذج الهجمات

ونموذج التعرف مبين في الشكل (٣-٥)



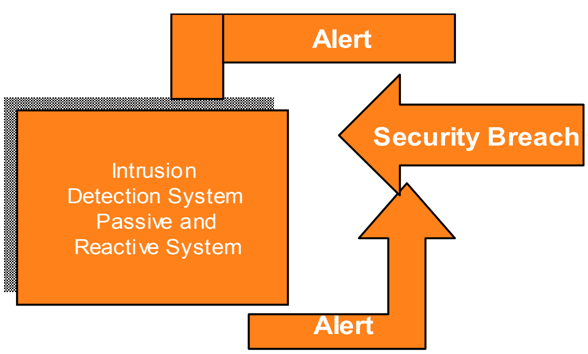
الشكل (٣-٥) يوضح نموذج التعرف [17]

٣-١-٣-٢ الفرق بين نظامي NIDS and HIDS

هناك نموذجان من IDS هما النموذج الشبكي NIDS والثاني المستقل host-based intrusion and detection system المعروف بـ HIDS و كلاهما يحلل الرزم في الشبكة ويقوم NIDS باكتشاف الرزم التي تعبر قواعد الفلترة في جدار النار اما HIDS فيختبر النشاطات في كل حاسب مستقل أو مضيف .

٣-١-٣-٣ الانظمة الخاملةوالأنظمة التفاعلية Passive and reactive systems

ان نظام IDS الخامل يكتشف الثغرات الكامنة في أمن الشبكة ويسجل الملاحظات ويرسل التنبيهات ثم يقوم النظام التفاعلي بالاستجابة لهذه النشاطات المشبوهه بواسطة اخراج المستخدم من العمل أو بواسطة برمجة سريعة لجدار النار لقفل تدفق الشبكة من جهة هذا النشاط. والشكل (٣-٦) يبين طريقةعمل الأنظمة الخاملة والتفاعلية .



الشكل (٣-٥) يوضح طريقة عمل الأنظمة الخاملة والنشطة [16]

٣-٣-٢ الفر ق بين جدار النار نظام كشف الاختراق IDS Firewall and IDS

يقوم جدارالنار بالبحث عن المخترقين لوقف الهجوم ومنعه من الحدوث ولهذا يقيد جدار النار الوصول بين الشبكات لوقف الدخلاء ولكن لايقوم الجدار بمعرفة المهاجم من داخل الشبكة نفسها وانما من خارج الشبكة فقط .

اما نظام التتبع فيختبر الدخلاء حال حدوث الهجوم وخاصة من داخل الشبكة التي يراقبها وخاصة انه في الشبكات اللاسلكية يظهر الدخلاء كانهم من داخل الشبكة وهذا يجعل من اكتشافهم مسالة معقدة . .[16]

الفصل الرابع

تحليل التشكيلات الأمنية للشبكات WLAN

مقدمة : يدخل في بناء نظام أمن الشبكات WLAN معدات وأجهزة وبرامج لكل منها مساهمتها في التأثير على سوية النظام الأمني .

٤-١ تحليل أمن الشبكات الحاسوبية اللاسلكية

تقيم العوامل المؤثرة في تماسك بنية النظام الأمني للشبكات WLAN إلى قسمين :

- أنظمة الترميز والتشفير ولوائح التحكم بالوصول ACL
- التجهيزات والمعدات ، مثل مخدمات المصادقة RADIUS ومخدمات التحكم بالمجال أو الجدران النارية أو أنظمة DMZ .

تلعب نقطة الوصول دورا هاما ومحوريا في تشكيلات النظام الأمني للشبكات WLAN في الواجهة الرئيسية للدخول الى الشبكة وتصنع بتقنيات متنوعة اذ تحوي ذاكرة مضمنة بمجموعة من البرامج قابلة للتطوير والترقية باستمرار لتدارك الاخطاء التي تظهر مع مرور الزمن ولاشك أن مسالة التوافق بين التجهيزات وبرامجها وعملية تطويرها يؤثر على أمن الشبكات WLAN خاصة بعد أن تصبح هذه التجهيزات قديمة بعض الشيء لذلك لابد من التركيز على هذه الناحية ودراسة البرامج المستخدمة من فترات سابقة والبرامج الحالية لتحديد الطريقة المناسبة لتطوير أمن الشبكة بكلفة معقولة .

ان العوامل المؤثرة على أمن الشبكات WLAN يمكن تلخيصها على النحو التالي :

- **بروتوكول التشفير المستخدم :** وهو بدوره يؤثر على مجموعة من البارامترات وهي:
  - زمن المصادقة
  - عدد الرسائل المتبادلة بين الزبون ونقطة الوصول

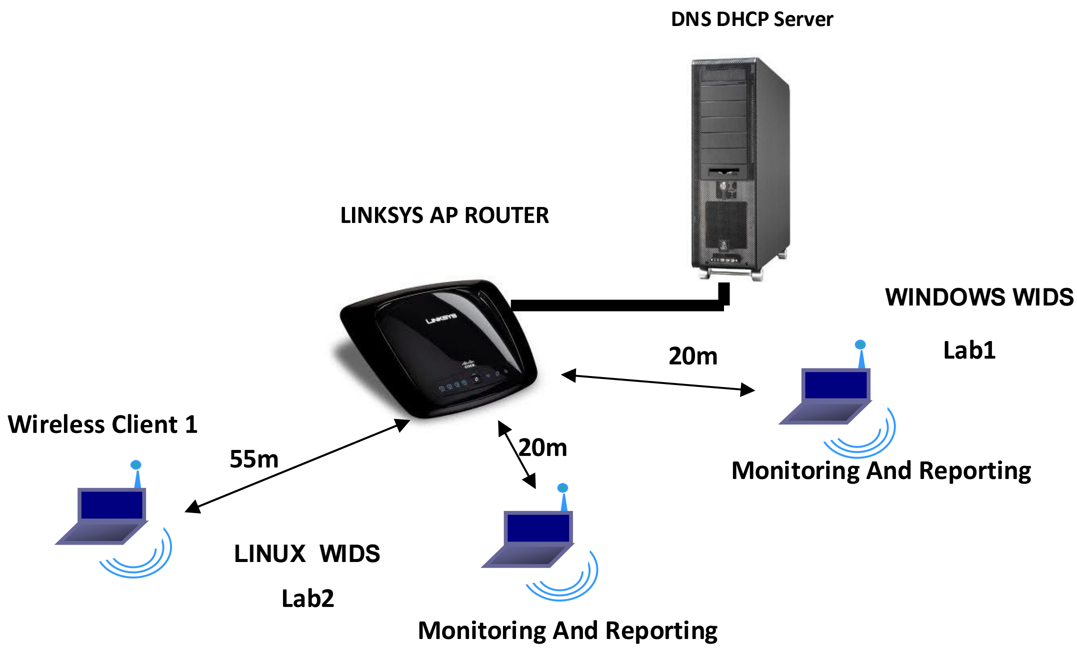
- الانتاجية
- زمن كسر التشفير
- عدد الباكيتات الملتقطة لكسر التشفير

➢ **مجموعة المخدمات المستعملة مثل مخدم المصادقة RADIUS و مخدم تحكم بالمجالDC** وهي تؤثر على مجموعة البارامترات السابقة نفسها

آخذين بعين الاعتبار العوامل السابقة تم بناء مجموعة من التشكيلات الأمنية ودراسة مدى تأثر هذه البارامترات بذلك .

وهذ السيناريوهات هي :

السيناريو الأول S1: يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٤-١) ويهدف السيناريو الى اختبار نقطة الوصول بدون نظام تشفير مع وجود مخدم تحكم مجال DNS وبروتوكول لتوزيع عناوين الشبكة DHCP حيث تعتبر قيم بارامتراته مرجعية لعدم وجود تشفير وعدم وجود مشاركة بالحزمة

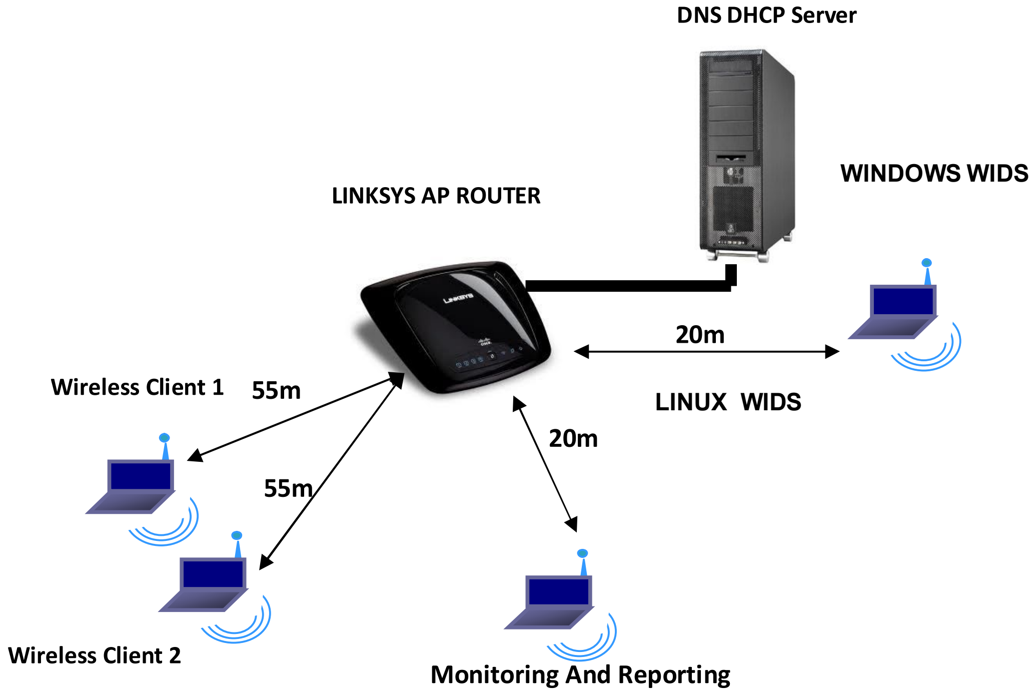


الشكل (٤-١) مكونات السيناريو الأول

وللوصول الى هذا السيناريو تم ضبط إعداد نقطة الوصول من جهة التشفير على WEP بدون كلمة سر (مصادقة مفتوحة) عبرمخدم مجال وبالتالي أصبح الوصول للنقطة يتم عبر اسم الشبكة اللاسلكية وبدون مصادقة ولكن تم تفعيل منح عناوين IP للزبون اللاسلكية عن طريق مخدم DHCP SEREVR وتم ايقاف منح العناوين المنطقية عن طريق نقطة الوصول نفسها .

كذلك تم اختبار الدخول للمجال اللاسلكي عن طريق Wirless Client 1 الذي يبعد عن نقطة الوصول مسافة 55 متر وتم مراقبة الدخول عن طريق Lab1 الذي يبعد عن نقطة الوصل مسافة 20 متر والمزود بنظام تشغيل windows 7 وبرنامجي wireshark و netsumbler و Lab2 الذي يبعد عن نقطة الوصول مسافة 20M وزود بنظام تشغيل LINUX Obunto وبرنامج Kismet الذي يعمل W IDS .

◄ السيناريو الثاني S2: يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٤-٢) الهدف من هذا السيناريو اختبار نقطة الوصول بدون نظام تشفير مع وجود مخدم تحكم مجال وبروتوكول توزيع عناوين الشبكة DHCP ومشاركة بالحزمة

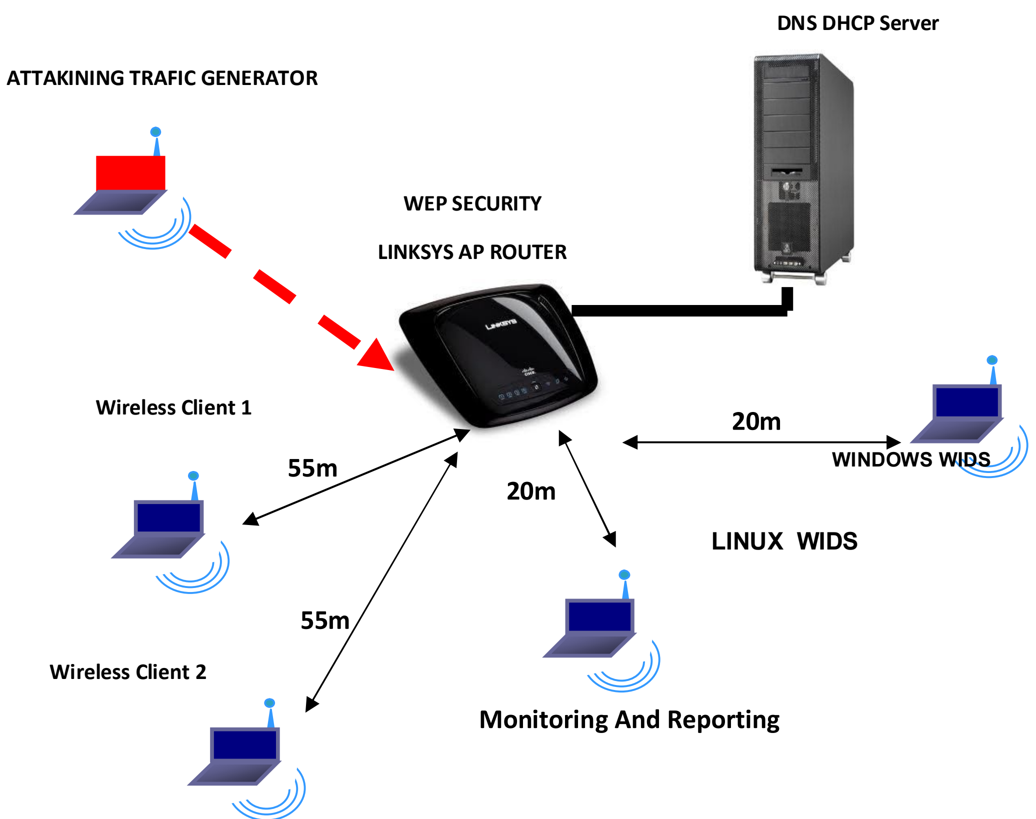


الشكل (٤-٢) مكونات السيناريو الثالث

وللوصول الى هذا السيناريو تم ضبط إعداد نقطة الوصول من جهة التشفير على WEP بدون كلمة سر وعن طريق مخدم تحكم بالمجال وبالتالي أصبح الوصول للنقطة يتم عبر اسم الشبكة اللاسلكية وبدون مصادقة ولكن تم تفعيل منح عناوين IP للزبون اللاسلكية عن طريق التوزيع الداخلي FIRMWARE والهدف من ذلك هو اختبار تأثير استخدام هذه الخدمة على الزبون اللاسلكي وخاصة زمن وعدد رسائل المصادقة

تم اختبار الدخول للمجال اللاسلكي عن طريق Wirless Client 1 الذي يبعد عن نقطة الوصول مسافة 55m و Wirless Client 2 الذي يشاركه بالحزمة ويبعد نفس البعد عن النقطة وتم مراقبة الدخول عن طريق Lab1 الذي يبعد عن نقطة الوصل مسافة 20M والمزود بنظام تشغيل 7 windows وبرنامجي wireshark و netsumbler و Lab2 الذي يبعد عن نقطة الوصول مسافة 20M وزود بنظام تشغيل LINUX Obunto وبرنامج Kismet الذي يعمل W IDS .

السيناريو الثالث S3 : يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٤-٣) الهدف من هذا السيناريو اختبار نقطة الوصول مع مخدم DNS +DHCP مع نظام تشفير WEP 64BIT



الشكل (٤-٣) مكونات السيناريو الرابع

وللوصول الى هذا السيناريو تم ضبط إعداد نقطة الوصول من جهة التشفير على WEP مع كلمة سر مؤلفة من 10 Character

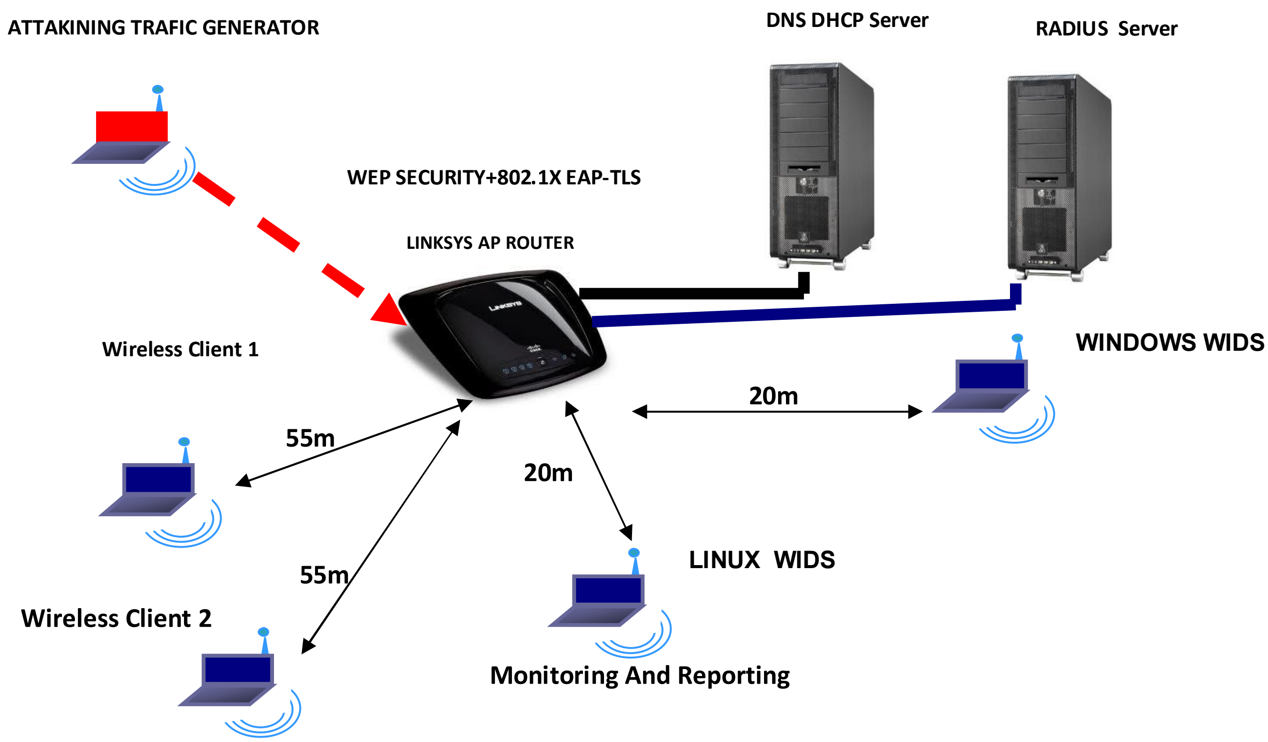
وبالتالي أصبح الوصول للنقطة يتم عبر اسم الشبكة اللاسلكية مع مصادقة ولكن تم تفعيل منح عناوين IP للزبون اللاسلكية عن طريق مخدم توزيع DHCP Server .

تم اختبار الدخول للمجال اللاسلكي عن طريق Wirless Client 1 الذي يبعد عن نقطة الوصول مسافة 55m وتم مراقبة الدخول عن طريق Lab1 الذي يبعد عن نقطة الوصل مسافة 20m والمزود بنظام تشغيل windows 7

وبرنامجي wireshark و netsumbler و Lab2 الذي يبعد عن نقطة الوصول مسافة 20M وزود بنظام تشغيل LINUX Obunto وبرنامج Kismet الذي يعمل W IDS .

وقد أضفناالحاسب Lab 3 فهو حاسب مزود بنظام تشغيل windows 7 وبرامج كسر شيفرة مثل Kismet الهدف منه التقاط باكيتات من المجال اللاسلكي لتحليلها ومعرفة الشيفرة .

السيناريو الرابع S4 : يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٤-٤) الهدف من هذا السيناريو اختبار نقطة الوصول مع مخدمين RADIUS و DNS+ DHCPمع نظام تشفير WEP واستخدام المعيار 802.1X ومع وجود مشاركة في الحزمة .



الشكل (٤-٤) مكونات السيناريو الخامس

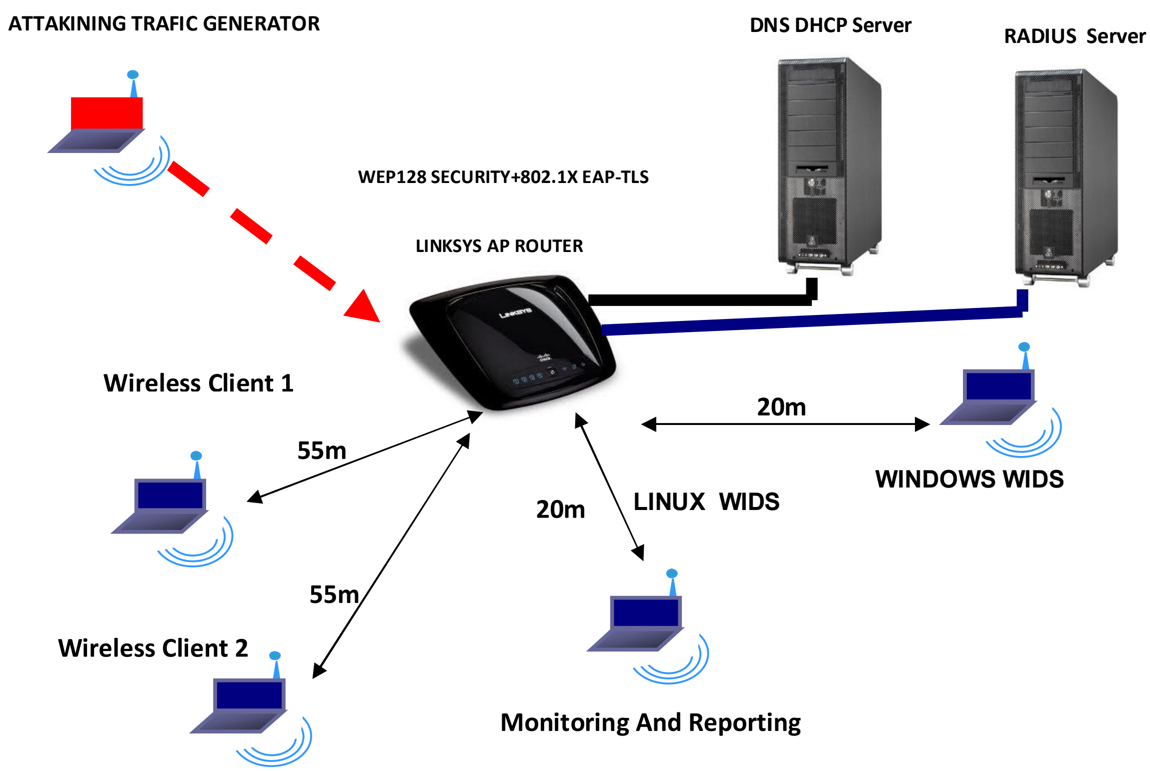
وللوصول الى هذا السيناريو تم ضبط إعداد نقطة الوصول من جهة التشفير على WEP مع كلمة سر مؤلفة من 10 Character

وبالتالي أصبح الوصول للنقطة يتم عبر اسم الشبكة اللاسلكية مع مصادقة ولكن تم تفعيل منح عناوين IP للزبون اللاسلكية عن طريق مخدم توزيع DNS Dhcp Server و RADIUS Server وباستخدام المصادقة عبر المعيار 802.1x والهدف من ذلك هو اختبار تأثير استخدام هذه المخدمات على على الزبون اللاسلكي .

تم اختبار الدخول للمجال اللاسلكي عن طريق Wirless Client 1 و Wirless Client 2 اللذين يبعدان عن نقطة الوصول مسافة 55m وتم مراقبة الدخول عن طريق Lab1 الذي يبعد عن نقطة الوصل مسافة 20M والمزود بنظام تشغيل windows 7 وبرنامجي wireshark و netsumbler و Lab2 الذي يبعد عن نقطة الوصول مسافة 20M وزود بنظام تشغيل LINUX Obunto وبرنامج Kismet الذي يعمل W IDS .

أما Lab 3 فهو حاسب مزود بنظام تشغيل windows 7 وبرامج كسر شيفرة مثل Kismet الهدف منه التقاط باكيتات من المجال اللاسلكي لتحليلها ومعرفة الشيفرة .

السيناريو الخامس S5 : يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٤-٥) الهدف من هذا السيناريو اختبار نقطة الوصول مع مخدم RADIUS و DNS+ DHCP مع نظام تشفير WEP 128BIT واستخدام المعيار 802.1X



الشكل (٤-٥) مكونات السيناريو التاسع

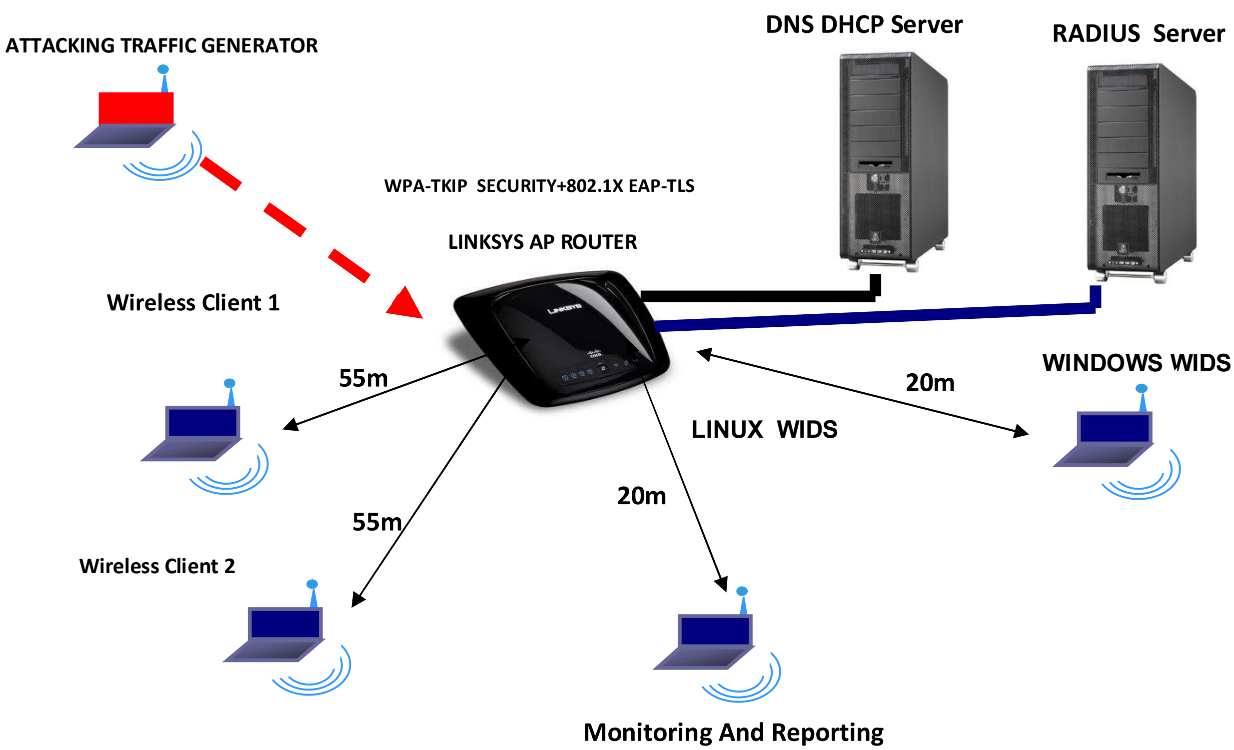
وللوصول الى هذا السيناريو تم ضبط إعداد نقطة الوصول من جهة التشفير على WEP 128 مع كلمة سر مؤلفة من 10 Character

وبالتالي أصبح الوصول للنقطة يتم عبر اسم الشبكة اللاسلكية مع مصادقة ولكن تم تفعيل منح عناوين IP للزبون اللاسلكية عن طريق مخدم توزيع DHCP SERVER و RADIUS Server وباستخدام المصادقة عبر المعيار 802.1x .

تم اختبار الدخول للمجال اللاسلكي عن طريق Wirless Client 1 و Wirless Client 2 اللذين يبعدان عن نقطة الوصول مسافة 55m وتم مراقبة الدخول عن طريق Lab1 الذي يبعد عن نقطة الوصل مسافة 20M والمزود بنظام تشغيل windows 7 وبرنامجي wireshark و netsumbler و Lab2 الذي يبعد عن نقطة الوصول مسافة 20M وزود بنظام تشغيل LINUX Obunto وبرنامج Kismet الذي يعمل W IDS .

أما Lab 3 فهو حاسب مزود بنظام تشغيل windows 7 وبرامج كسر شيفرة مثل Kismet الهدف منه التقاط باكيتات من المجال اللاسلكي لتحليلها ومعرفة الشيفرة .

◄ السيناريو السادس S6 : يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٤-٦) الهدف من هذا السيناريو اختبار نقطة الوصول مع مخدم RADIUS و DHCP DNS مع نظام تشفير 128BIT WPA TKIP واستخدام المعيار 802.1X .



الشكل (٤-٦) مكونات السيناريو العاشر

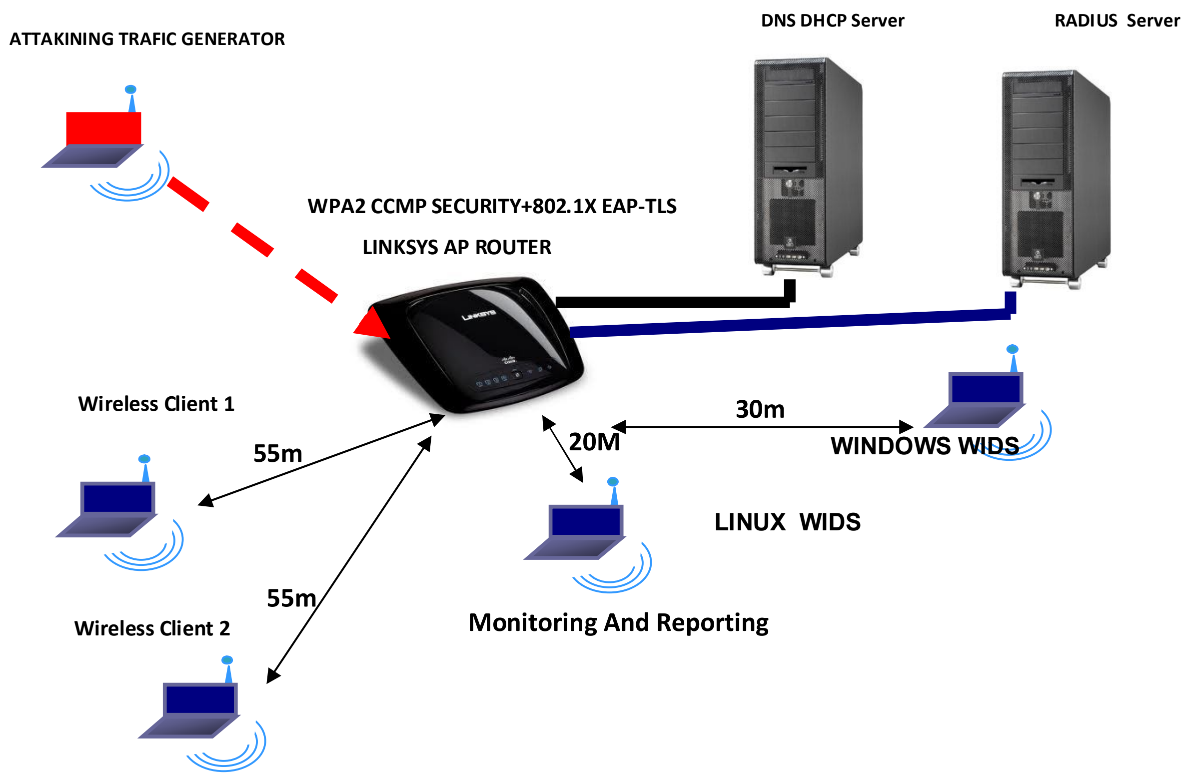
وللوصول الى هذا السيناريو تم ضبط إعداد نقطة الوصول من جهة التشفير على WPA 128 مع بروتوكول تبديل المفاتيح الديناميكي TKIP كلمة سر مؤلفة من 10 Character وبالتالي أصبح الوصول للنقطة يتم عبر اسم

الشبكة اللاسلكية مع مصادقة ولكن تم تفعيل منح عناوين IP للزبون اللاسلكية عن طريق مخدم تحكم كجال وبروتوكول توزيع DHCP SERVER و RADIUS Server وباستخدام المصادقة عبر المعيار 802.1x اضافة الى ضبط الدخول عن طريق لوائح الوصول ACCESS LIST والمكونة من ثمانية عناوين فيزيائية من بينها عنواني الزبونين اللاسلكيين WC1 وWC2 والهدف من ذلك هو اختبار تأثير استخدام هذه المكونات على الزبون اللاسلكي .

تم اختبار الدخول للمجال اللاسلكي عن طريق Wirless Client 1 و Wirless Client 2 اللذين يبعدان عن نقطة الوصول مسافة 55m وتم مراقبة الدخول عن طريق Lab1 الذي يبعد عن نقطة الوصل مسافة 20M والمزود بنظام تشغيل windows 7 وبرنامجي wireshark و netsumbler و Lab2 الذي يبعد عن نقطة الوصول مسافة 20M وزود بنظام تشغيل LINUX Obunto وبرنامج Kismet الذي يعمل W IDS .

أما Lab 3 فهو حاسب مزود بنظام تشغيل windows 7 وبرامج كسر شيفرة مثل Kismet الهدف منه التقاط باكيتات من المجال اللاسلكي لتحليلها ومعرفة الشيفرة

السيناريو السابع S7 : يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٤-٧) الهدف من هذا السيناريو اختبار نقطة الوصول مع مخدم RADIUS و DHCP DNS مع نظام تشفير WPA2-CCMP 128BIT واستخدام المعيار 802.1X



الشكل (٤-٧) مكونات السيناريو السابع

وللوصول الى هذا السيناريو تم ضبط إعداد نقطة الوصول من جهة التشفير على WPA2 128 مع بروتوكول CCMP كلمة سر مؤلفة من 10 Character وبالتالي أصبح الوصول للنقطة يتم عبر اسم الشبكة اللاسلكية مع مصادقة محددة بوصول مقيد ولكن تم تفعيل منح عناوين IP للزبون اللاسلكية عن طريق مخدم DHCPو RADIUS Server وباستخدام المصادقة عبر المعيار 802.1x والهدف من ذلك هو اختبار تأثير استخدام هذه المخدمات على على الزبون اللاسلكي .

تم اختبار الدخول للمجال اللاسلكي عن طريق Wirless Client 1 و Wirless Client 2 اللذين يبعدان عن نقطة الوصول مسافة 55m وتم مراقبة الدخول عن طريق Lab1 الذي يبعد عن نقطة الوصل مسافة 20M والمزود بنظام تشغيل windows 7 وبرنامجي wireshark و netsumbler و Lab2 الذي يبعد عن نقطة الوصول مسافة 20M وزود بنظام تشغيل LINUX Obunto وبرنامج Kismet الذي يعمل W IDS .

أما Lab 3 فهو حاسب مزود بنظام تشغيل windows 7 وبرامج كسر شيفرة مثل Kismet الهدف منه التقاط باكيتات من المجال اللاسلكي لتحليلها ومعرفة الشيفرة

٤–٢ الأدوات المستخدمة للمراقبة والتحليل

Monitor and Analysis tools

تتنوع الادوات المستخدمة في مراقبة وتحليل الشبكة بين برمجيات شركات غالية الثمن وبرامج مجانية بعضها مفتوحة المصدر ومشكلة بعض برامج الشبكات اللاسلكية أنها سلاح يستخدمه العدو والصديق لاكتشاف الشبكات اللاسلكية [12]

حيث انها تمكن مديري الشبكات الكبيرة أو المستخدمين في المنزل الحصول على مسح للأجواء سعيا وراء التقاط الإشارات اللاسلكية وحركة البيانات في الشبكات اللاسلكية المحلية WLAN ومواقعها .

ورغم الجهود الكبيرة للشركات والمطورين وهيئات المعايير المجانية إلا أن حماية الشبكات اللاسلكية بصورة محكمة لاتزال بعيدة المنال ويعود السبب الرئيس في ذلك الى ان بروتوكولات الحماية لا تخلو حتى الآن من ثغرات ، اضافة الى المستخدمين الذين لا يأبهون لضرورة ضبط إعدادات الحماية. ولذلك فإن تحليل حركة البيانات في الشبكات اللاسلكية واستكشاف مجال تغطية هذه الشبكات اللاسلكية هو أمر ضروري يمكن تنفيذه بسهولة من قبل المختصين ومديري الشبكات اللاسلكية العاملة

٢–٤ –١ أدوات وبرامج القياس Measurment Tools:

يتوفر مجموعة متنوعة من البرامج المؤهلة لقياس البارمترات اللازمة ، من هذه البرامج :

❶ برنامج Wireshark :

وكان يسمى سابقا بـ Ethereal وهو ملتقط باكيتات موزعة يعمل كمحلل بروتوكول protocol analyzer وقد استخدمناه لقياس عدد رسائل المصادقة وزمن المصادقة .

❷ برنامج **IPREF** :

وهي أداة فعالة للقياس في طبقة النقل Transport Layer لكل من TCPو UDP وهو يعمل بنظام Client Server – ويسجل عرض الحزمة والتاخير ويستخدم طريقة نقل البيانات من الذاكرة للذاكرة Memory to Memory من مضيف الزبون الى مضيف المخدم حيث يقوم المخدم بالاستماع الى منفذ TCP للزبون وهذا يسمح ببدء القياس لحظة اتصال الزبون .

❸ برنامج **Kismet** :

وهو برنامج اكتشاف وتتبع للدخلاء يعمل بطريقة Snifer ويولد انذارات مبرمجة Alerts في قاعدة بيانات داخلية عند اكتشاف هجمات أو متطفلين وهو يصنف ضمن برامج Wireless Intudion Detection Systems (WIDS) . يقدم برنامج كسمت kismet وهو برنامج التقاط إشارات الطبقة ٢ في الشبكات اللاسلكية والذي يكشف محاولات الاختراق ويعمل مع أي بطاقة اتصال لاسلكي تدعم وضعية مراقبة البيانات ويكشف حركة البيانات في شبكات لاسلكية تعمل بمعيار WI-FI بأنواعه التالية (802.11b, 802.11a, and 802.11g traffic) ويحدد البرنامج وجود تلك الشبكات من خلال جمع كتل البيانات وتحديد أسمائها حتى إن كانت مخفية nonbeaconing networksمن خلال حركة البيانات. ويمكن استخدام البرنامج خلال التنقل بصورة مسح خامل passive scanning لاستكشاف وجود الشبكات اللاسلكية أو استخدامه بصورة ثابتة للمراقبة المتواصل لحال الشبكة. ويختلف كسمت عن غيره من برامج هذه الفئة التي تستكشف مكان الشبكات اللاسلكية ، في أنه لا يسعى للاتصال ببر نامج بطاقة الاتصال اللاسلكي الخاص بالتعامل مع الشبكات اللاسلكية firmware (وهو برنامج يتيح للبطاقة اكتشاف الشبكات اللاسلكية الموجودة بتحليل الإشارات التي تبثها). حيث يقوم كسمت بجمع كل كتل البيانات الموجودة في الهواء في أي لحظة ويحدد مصدرها من الشبكات المتعددة إن وجدت. ويمكنه بذلك كشف الشبكات ذات معرفات الخدمة المخفية Hidden SSIDs ، وفي حال توفر نظام تحديد المواقع GPS يمكن للبرنامج تسجيل إحداثيات موقع كل كتلة يلتقطها. وفي حال توفر ملف خريطة رقمية لذلك النظام يقوم كسمت بتحديد موقع الشبكة اللاسلكية التي يلتقط إشاراتها على الخريطة بفضل أداة خاصة في البرنامج اسمها.gpsmap

❹ برنامج **Netstumbler** :

هو أحد أوائل البرامج الخدمية الخاصة بالشبكات اللاسلكية وهو من فئة برامج الاستكشاف sniffer ، ويماثل كسمت في أنه يسمح للمستخدمين باكتشاف شبكات لاسلكية WI-FI بمعياري A و-802.11a - 802.11b) B (802.11nلكن هذا يعمل في ويندوز .كما يظهر البرنامج نقاط النفاذ وبيانات أخرى مثل هويات تعريف الاجهزة SSIDوالأقنية ويمكنه كشف وجود تشفير من نوع WEP في حال كان الأخير نشطا أو معطلا. ويضم نت ستمبلر القدرة على التكامل مع أجهزة تحديد المواقع GPS لتحديد مكان الشبكات التي يكتشفها، ومؤشرات قوة إشارات الشبكة اللاسلكية.ويستخدم البرنامج من قبل بعض الشركات الكبيرة التي ترغب بإجراء تدقيق أمن لشبكاتها اللاسلكية والتجول في نطاقها لضمان عمل التشفير في كل نقاط النفاذ فيها، إلى جانب التأكد من توفر تعريف محدد وفريد SSID لكل من الأجهزة. كما يمكن استخدام البرنامج لمهام الإدارة أيضا مثل تحديد جودة الإشارة اللاسلكية في منطقة تغطية الشبكة اللاسلكية والتعرف على أفضل توجيه للهوائيات.
ويتميز نت ستمبلر بأنه سهل الاستخدام على النقيض من برنامج كسمت، كما أنه يقوم بمهام المسح النشط active

scanningأي أنه يتدخل في عمل الشبكة بحيث يبث إشارة سبر لها (broadcast probes) على كل الأقنية وعندما تستجيب له أي نقطة نفاذ يتم التقاطها، وتبلغ نسبة الشبكات التي تمت تهيئتها لعدم الاستجابة حوالي ٥٠ %

٢-٤-٢ التجهيزات المستخدمة في الاختبار Wireless Test Lab Configuration:

١- مخدم SERVER عدد /١/ : هو حاسب مزود بظام تشغيل Microsoft Windows Server 2003 Enterprise Editon named DC والذي يعمل كمخدم مجال DNS ومزود باعدادات بروتوكول DHCP

٢- حاسب Labtop عدد /٢/ تعمل كزبائن لاسلكية Wireless Clients .

٣- مخدم RADIUS SERVER عدد/١/ : وهو حاسب مزود بنظام تشغيل W2003 SERVER وهو مزود بخدمة Remote Autentication Dial in User Service .

٤- نقطة وصول Access Point نوع LINKSYS من النوع 802.11 G مزودة بموجه وموزع IP الي داخل DHCP FIRMWARE .

٥- حاسب Lab1 عدد /١/ مزود بنظام تشغيل windows 7 Ultimate يعمل كمراقب ومسجل للأحداث في المجال اللاسلكي

٦- حاسب Lab2 عدد/١/ مزود بنظام تشغيل LINUX Obunto يعمل كمراقب ومسجل للأحداث في المجال اللاسلكي

٧- حاسب Lab3 عدد /١/ مزود بنظام تشغيل LINUX Obunto يعمل كمولد هجمات لاسلكية.

والجدول (٤-١) يبين مواصفات أجهزة الحواسيب المستخدمة في اجراء التجارب

اسم الجهاز	LAB1	LAB2	LAB3	DNS/DHCP SERVER	RADIUS SERVER
الذاكرة الرئيسية	2GB	2GB	2GB	4GB	4GB
المعالج	CORE2 DUE 1.73GHZ	CORE2 DUE 1.73GHZ	I5 2.3GHZ	CORE2 DUE 1.73GHZ	CORE2 DUE 1.73GHZ
ذاكرة الكاش	2MB	2MB	3MB	2MB	2MB
كرت الشبكة	Atheros	Atheros	Atheros	D-LINK	D-LINK

10/100MBPS	**10/100MBPS**	**802.11 B/G**	**802.11 B/G**	**802.11 B/G**	

الجدول (١-٤)

الفصل الخامس

القياسات والنتائج

مقدمة :تشكل مرحلة القياس وتدقيق النتائج ، مرحلة هامة لتحديد خصوصية السيناريوهات المقترحة وبالتالي تحديد طريقة لكي يتم اعتمادها من قبل مديري الشبكات WLAN لقد ركزنا في القياسات على البارامترات المؤثرة في تحديد المستوى الأمني للشبكة

٥-١ بارامترات القياس تم اختبار خمس بارامترات لمختلف السيناريوهات المقترحة وهذه البارامترات هي :

❶ عدد الرسائل المتبادلة في المصادقة **Exchanged Authentication Messages** وهي مجموعة الرسائل المتبادلة بين الزبون اللاسلكي Wireless Client ونقطة الوصول AP ومايتصل بها وسنرمزلهذا البارامتر بـ **M**

❷ زمن المصادقة **Autentication Time** ويعرف بأنه الزمن المستغرق من أول رسالة طلب مصادقة مستقبلة من العميل الى حين اعطاء السماح بالدخول إلى الشبكة وسنرمز له بـ **A**

❸ الإنتاجية **Throughput** والمقصود بها انتاجية البروتوكول TCP حيث أن آلية التشفير المتبعة في السيناريو تؤثر على نقل المعلومات عبر الوصلة اللاسلكية .وانه بعد اتمام عملية المصادقة بنجاح وبعد اتمام تبادل المفاتيح فإن كل المعلومات المتدفقة عبر الشبكة سوف تشفر في الجلسة الحاليةوبالتالي تعبر عن انتاجية السيناريو ونرمزله بـ T

❹ زمن اختراق التشفير **Cracking Time** والمقصود به الزمن الذي يستغرقه برنامج كسر بروتوكول التشفير حتى يكسر فعليا و يعمل برنامج الاختراق بطريقة snifer ويعبر الزمن في هذه الحالة عن زمن اختراق التشفيرضمن هذا السيناريو ونرمز لهذا البارامتر بـ **C**

❺عدد الباكيتات اللازمة لكسر الشيفرة **Packets No** حيث يقوم برنامج القرصنه بالتجسس على المجال اللاسلكي ويجمع الباكيتات التي يحللها ليحصل على الشيفرة الخاصة بها . ويرمز لهذا المتغير بـ**P**

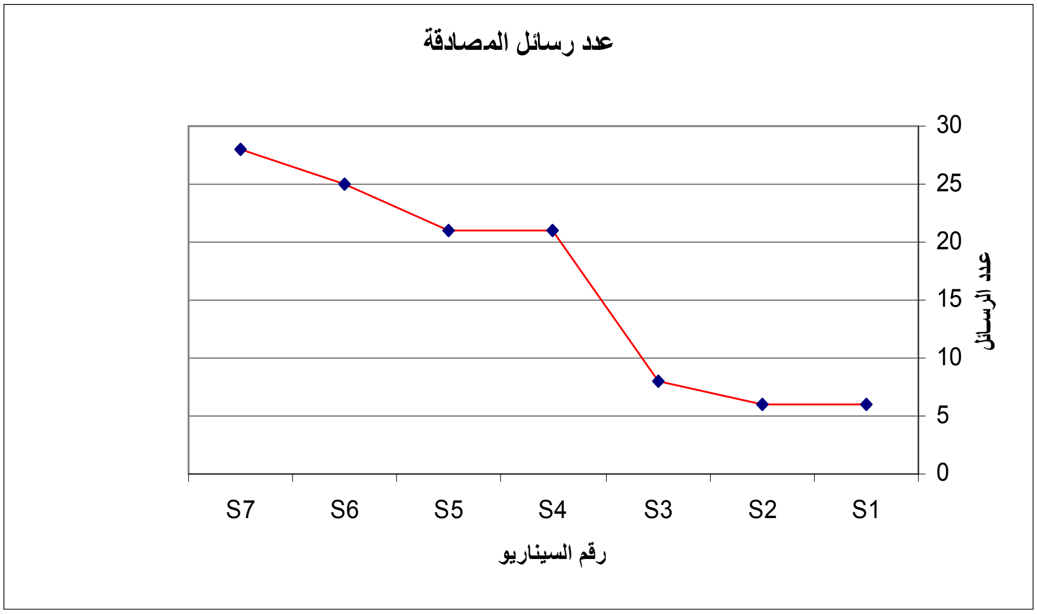
٥-١-١ عدد رسائل المصادقة المتبادلة Exchanged Autentication Message :

تم اختبار السيناريوهات من S1 الى S7 و اجراء ١٥ تجربة لكل سيناريو، و كانت النتائج كما في الجدول التالي (٥-١) يلي :

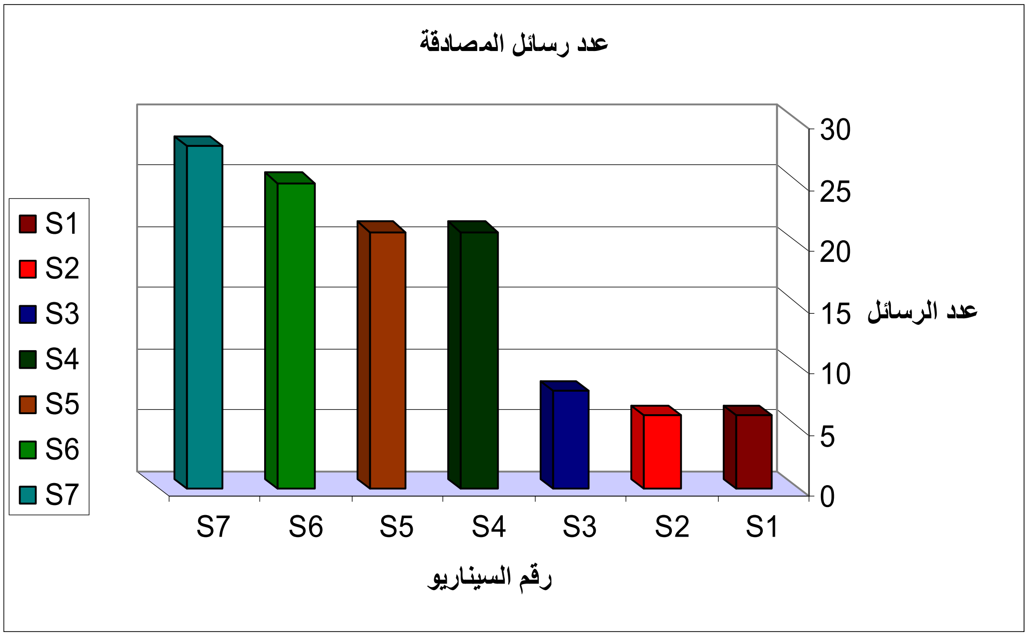
Scenario NO.	Scenario Description	NO. OF Autentication messages per client (M)
S1	Open System +DNS DHCP+WC1	٦
S2	Open System + DNS DHCP +wc1+wc2	٦
S3	Wep+ DNS DHCP +wc1+wc2	**8**
S4	Wep802.1x+ DNS DHCP +RADIUS+wc1+wc2	**21**
S5	Wep128-802.1x+ DNS DHCP +RADIUS+wc1+wc2	**21**
S6	Wpa802.1x + DNS DHCP +RADIUS+wc1+wc2	**25**
S7	Wpa2 -802.1x+ DNS DHCP ++RADIUS +wc1 +wc2	٢٨

الجدول (٥-١) يبين عدد رسائل المصادقة في السيناريوهات المختلفة

نلاحظ من الجدول السابق ازدياد عدد رسائل المصادقة بشكل كبير عند الانتقال من نظام أمني بسيط يعتمد فقط نقطة الوصول AP مثل S1,S2,S3 إلى نظام أمني أكثر تعقيدا مكون من مخدم مصادقة RADIUS بالإضافة الى استخدام المعيار 802.1X مع بروتوكول التشفير WEP64 كما في الحالة S4 ونلاحظ من خلال تحليل عدد رسائل المصادقة بين السيناريوهين S4وS5 والسيناريوهين S1و S2 هو وجود نفس عدد الرسائل بسبب ارتباطهما بنفس نوع بروتوكول التشفير (لايوجد تشفير في S1,S2 و WEP في S4,S5)ونلاحظ عدم ارتباط عدد رسائل المصادقة بطول مفتاح التشفير كما في حالة WEP 64 و WEP 128 في السيناريوهين S4,S5 على التوالي .يمكن رسم مخطط يبين العلاقة للسيناريوهات المدروسة مع تطور عدد الرسائل كما هو موضح في الشكل (٥-١) والشكل (٥-٢)



الشكل (٥-١) يبين عدد رسائل المصادقة في السيناريوهات المدروسة



الشكل (٥-٢) يبين عدد رسائل المصادقة في السيناريوهات المدروسة

٥-١-٢زمن المصادقة Authentication Time :

تم اختبار السيناريوهات من S1 حتى S7 من حيث زمن المصادقة بواسطة برنامج Wireshark وتم اجراء التجربة على كل سيناريو ١٥ مرة للحصول على القيم المتوسطة وكانت النتائج حسب الجدول (٥-٢) بالشكل التالي :

Scenario NO.	Scenario Description	Autentication Time in seconds A
S1	Open System +DHCP+WC1	0.064283
S2	Open System + DHCP +wc1+wc2	0.056324
S3	Wep+ DHCP +wc1+wc2	0.091875
S4	Wep802.1x+ DHCP +RADIUS+wc1+wc2	0.109325
S5	Wep128-802.1x+ DHCP +RADIUS+wc1+wc2	0.115243
S6	Wpa802.1x + DHCP +RADIUS+wc1+wc2	0.163621
S7	Wpa2 -802.1x+ DHCP ++RADIUS +wc1 +wc2	٠.212345

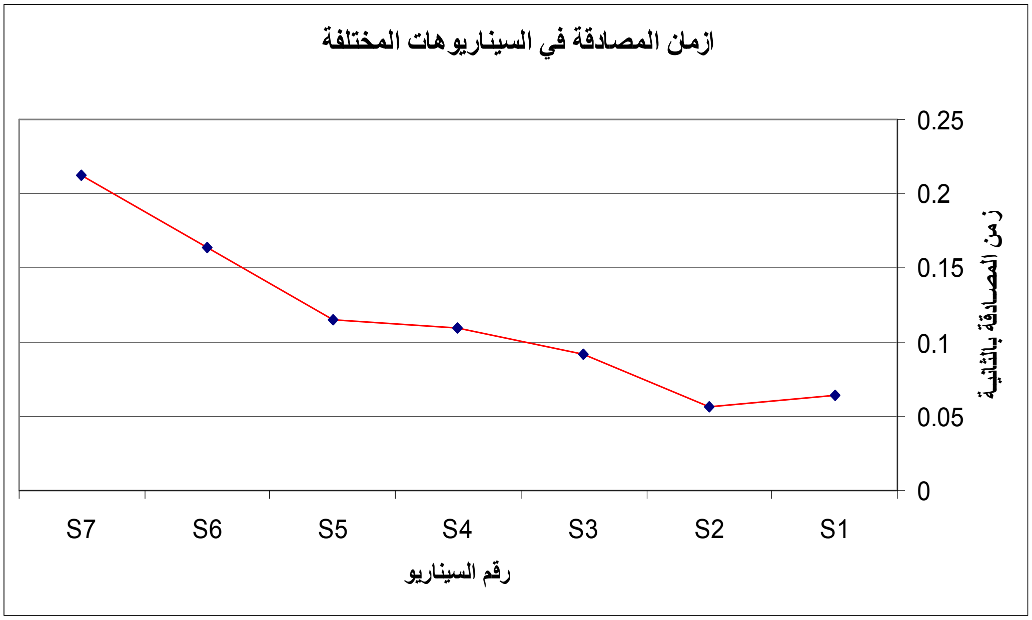
الجدول (٥-٢) يبين زمن المصادقة في السيناريوهات المختلفة

نلاحظ من تحليل الجدول (٥-٢) انه بالنسبة للسيناريوهات S1,S2,S3 التي تعتمد على نقطة وصول دون مخدم مصادقة أن أزمان المصادقة صغيرة بالمقارنة مع السيناريوهات الأخرى التي زاد فيها زمن المصادقة عدة مرات بتأثير وجود عبء ناتج عن الشبكة السلكية ومخدم المصادقة RADIUS (EAP و EAPOL).

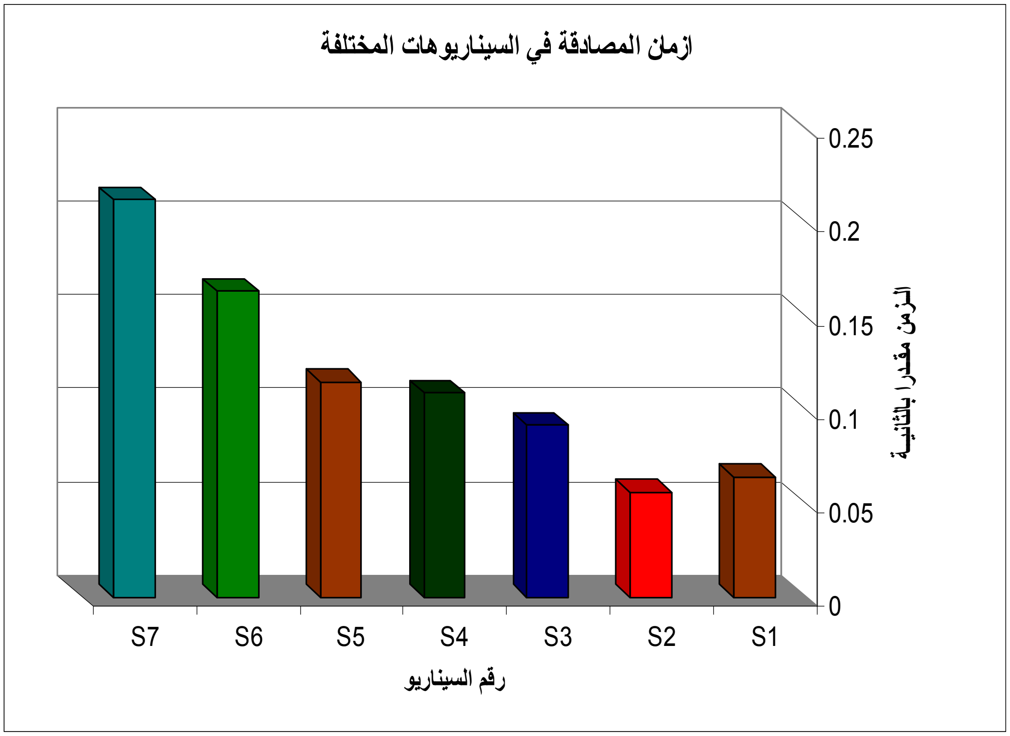
ومن تحليل الأزمان في السيناريوهات S4حتى S7 نجد ان نوع البروتوكول الأمني المستخدم يؤثر في ز من المصادقة بسبب آلية عمل البروتوكول .

يؤدي زيادة طول المفتاح لبروتوكول التشفير WEP من 64 في السيناريو S4 الى 128

في S5 الى زيادة بسيطه في زمن المصادقة أما الانتقال من بروتوكول WPA1 الى WPA2 فيؤدي لزيادة كبيرة لزمن المصادقة كما يظهر في الشكل (٥-٣) والشكل (٥-٤)



الشكل (٥-٣) يبن أزمنة المصادقة في السيناريوهات المدروسة



الشكل (٥-٤) يبن أزمنة المصادقة في السيناريوهات المدروسة

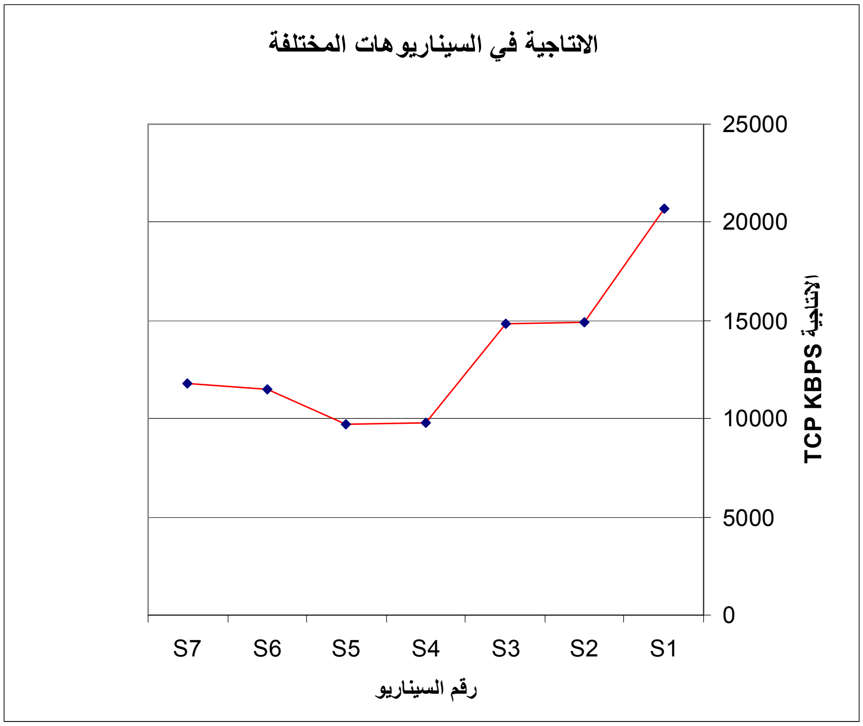
٣-٦-٣ انتاجية السيناريو Throughput:

تم اختبار السيناريوهات السابقة بالنسبة لانتاجية البروتوكول TCPعن طريق برنامج IPREF تم اجراء كل تجربة ١٥ مرة للحصول على القيم المتوسطة وهي موضحة بالجدول التالي :

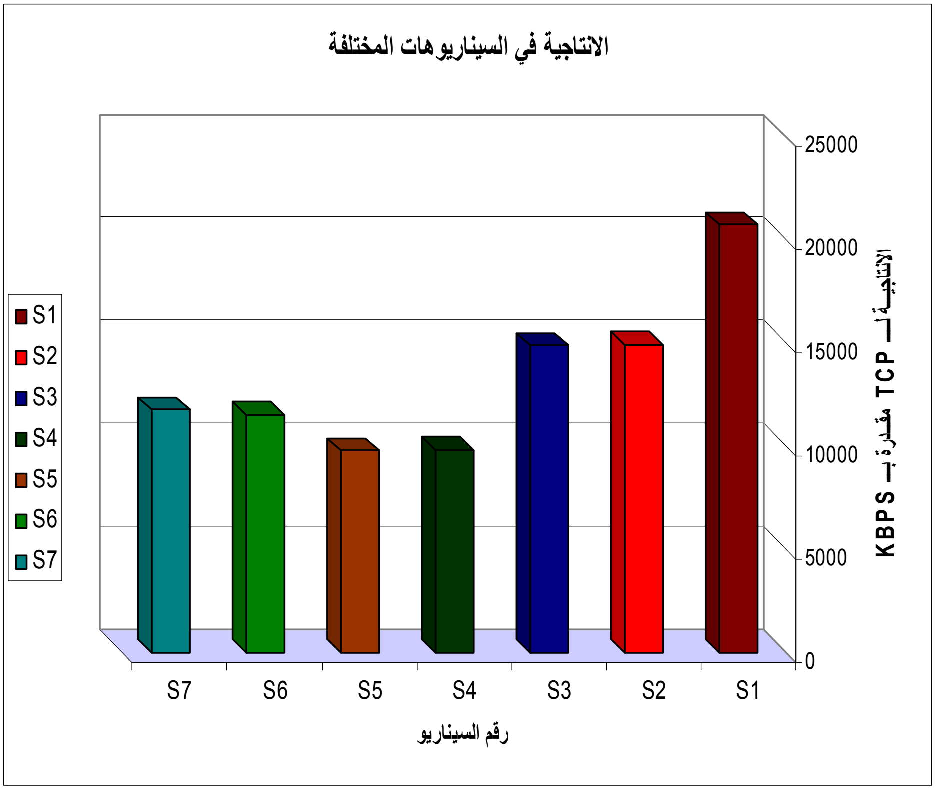
Scenario NO.	Scenario Description	TCP throughput in Kbps T
S1	Open System +DHCP+WC1	20705
S2	Open System + DHCP +wc1+wc2	١٤٨٩٣
S3	Wep+ DHCP +wc1+wc2	١٤٨٤٩
S4	Wep802.1x+ DHCP +RADIUS+wc1+wc2	٩٨١٩
S5	Wep128-802.1x+ DHCP +RADIUS+wc1+wc2	٩٧٤٦
S6	Wpa802.1x + DHCP +RADIUS+wc1+wc2	11518
S7	Wpa2 -802.1x+ DHCP ++RADIUS +wc1 +wc2	11766

الجدول (٥-٣) يبين عدد رسائل المصادقة في السيناريوهات المختلفة

نلاحظ من الجدول (٥-٣) انخفاضاًكبيراً في انتاجية البروتوكول TCP في حالة المشاركة في الحزمة في السيناريوهات الأمنية البسيطة مثل S1,S2,S3 كما نلاحظ انخفاضا بسيطا في الانتاجية في حالة استخدام بروتوكول WEP 64 كما في S3 أما في حالة السيناريوهات الأمنية الأكثر تعقيدا التي تحوي مخدمات مصادقة نلاحظ انخفاضا كبيرا في الانتاجية عن الحالة الأمنية البسيطة تصل حتى% ٣٤ أما استخدام بروتوكول التشفير WEPبمفتاح تشفير أطول ١٢٨ بدلا من 64 اثر بشكل بسيط في الانتاجية ونلاحظ أن مردود البروتوكول WPA مع TKIP هو أكبر من بروتوكول WEP ونلاحظ تقارب نتاجية البروتوكولين WPAو٢ WPAور بما يعود ذلك الى أن بروتوكول WPA2 يحتاج لمفتاح لكل بلوك معلومات مما يزيد تعقيد العملية ويخفض الانتاجية أما WPA1 فهو يحتاج الى مفتاح لكل ١٠٠٠٠ باكيت .يمكن تخطيطا توضيح تطور الانتاجية لمختلف السيناريوهات كما هومبين في الشكلين (٥-٥) و(٥-٦)



الشكل (٥-٥) يبن الانتاجية في السيناريوهات المدروسة



الشكل (٥-٦) يبن الانتاجية في السيناريوهات المدروسة

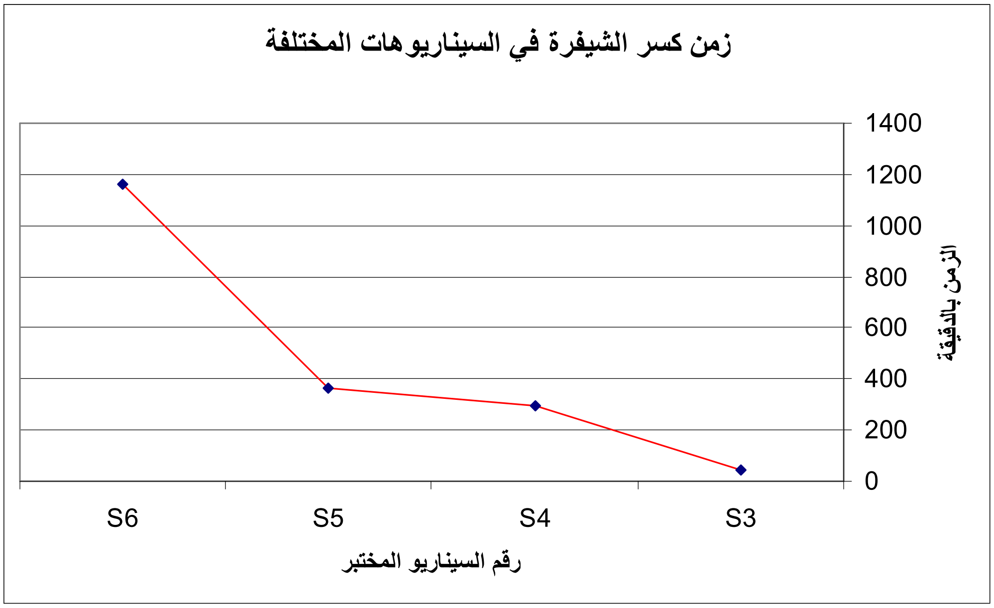
٣-٦-٤ زمن كسر مفتاح تشفير بروتوكول السيناريو Cracking Time:

تم اختبار السيناريوهات السابقة بالنسبة لزمن كسر البروتوكولات المختلفة بواسطة برنامج Kismet تم اجراء كل تجربة ١٥ مرة للحصول على القيم المتوسطة وهي موضحة بالجدول التالي :

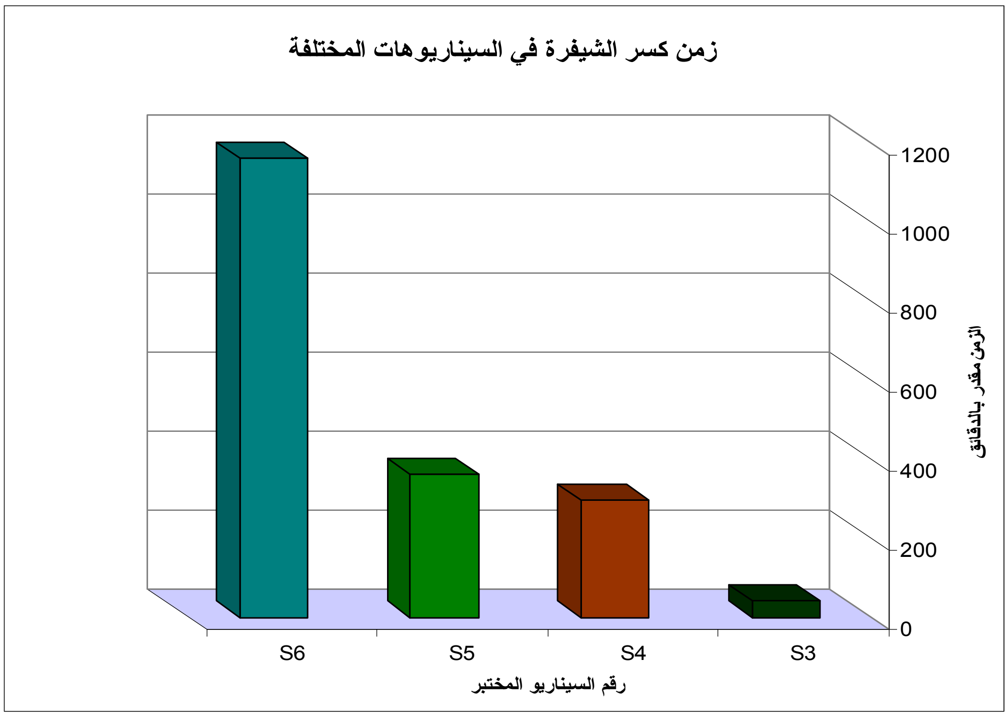
Scenario NO.	Scenario Description	Total time to crack security (minute) C
S1	Open System +DHCP+WC1	-
S2	Open System + DHCP +wc1+wc2	-
S3	Wep+ DHCP +wc1+wc2	42
S4	Wep802.1x+ DHCP +RADIUS+wc1+wc2	٢97
S5	Wep128-802.1x+ DHCP +RADIUS+wc1+wc2	٣36
S6	Wpa802.1x + DHCP +RADIUS+wc1+wc2	1163
S7	Wpa2 -802.1x+ DHCP ++RADIUS +wc1 +wc2	-

الجدول (٥-٤) يبين الزمن الكلي اللازم لكسر مفتاح تشفير بروتوكول للسيناريو

بالنسبة للسيناريوهات البسيطة كما في حالة S3 فنلاحظ ان زمن كسر مفتاح بروتوكول التشيفر بسيط أي أن التشفير من ناحية القوة الأمنية ضعيف وخاصة أن هذا السيناريو لايمتلك مخدم مصادقة يزيدقوته الأمنية , أما في حالة السيناريو S4 فنلاحظ أن زمن كسر الشيفرة يزيد بمقدار خمس مرات أما زيادة طول مفتاح بروتوكول التشفير WEP من 64الى ١٢٨ فيؤدي الى زيادة زمن كسر المفتاح بمعدل 30% أما في حالة تغيير نوع بروتوكول التشفير الى WPA فان زمن كسر الشيفرة يزيد بمقدار ٣ أضعاف على الأقل .أما بالنسبة للبروتوكول WPA2 فلايوجد هجوم معروف حتى الأن لاختراقه . الشكلين (٥-٧)و(٥-٨) يبين النتائج تخطيطا.



الشكل (٥-٧) يبن زمن كسر الشيفرة في السيناريوهات المدروسة



الشكل (٥-٨) يبن زمن كسر الشيفرة في السيناريوهات المدروسة

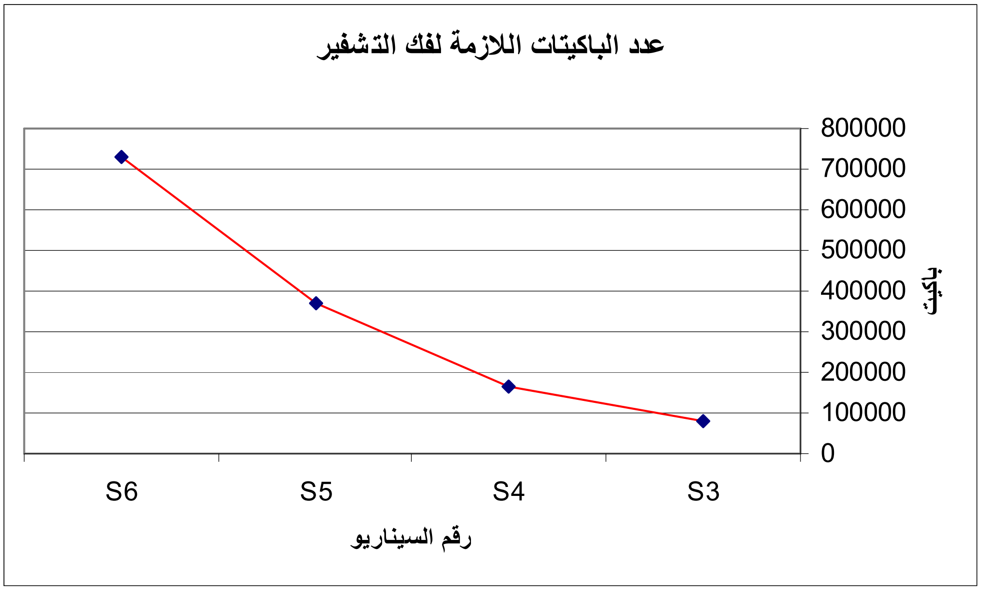
٣-٦-٥ عدد الباكيتات اللازمة لكسر المفتاح لبروتوكول التشيفر Packets NO :

تم اختبار السيناريوهات السابقة بالنسبة لعدد الباكيتات الملتقطة لكسر مفتاح بروتوكولات التشفير عن طريق برنامج Kismet تم اجراء كل تجربة ١٥ مرة للحصول على القيم المتوسطة وهي موضحة بالجدول التالي :

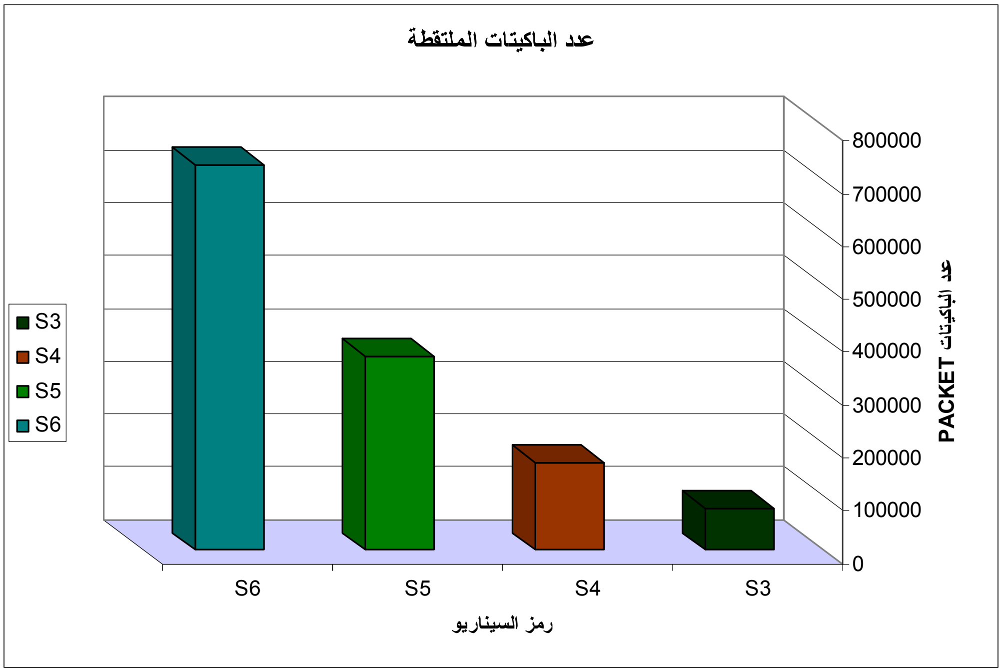
Scenario NO.	Scenario Description	NO.F packets/frames to complete crack P
S1	Open System +DHCP+WC1	-
S2	Open System +dhcp+wc1+wc2	-
S3	Wep+dhcp+wc1+wc2	**78000**
S4	Wep802.1x+dhcp+RADIUS+wc1+wc2	**167000**
S5	Wep128-802.1x+dhcp+RADIUS+wc1+wc2	**368000**
S6	Wpa802.1x +dhcp+RADIUS+wc1+wc2	**730000**
S7	Wpa2 -802.1x+dhcp++RADIUS +wc1 +wc2	-

الجدول (٥-٥) يبين عدد الباكيتات اللازمة لكسر مفتاح بروتوكول التشفير في السيناريوهات المختلفة

نلاحظ من الجدول السابق ازدياداُكبيراً في عددالباكيتات اللازمة لكسر الشيفرة بين السيناريو الأمني البسيط S3 والسيناريوهات الاكثر تعقيدا التي تحتوي على مخدمات مصادقة RADIUS وهذا يدل على أن دور مخدم المصادقة في زيادة القوة الأمنية للسيناريو كما نلاحظ أن استخدام البروتوكول WPA مع TKIP يؤدي لزيادة القوة الأمنية بشكل كبير وخاصة اذا علمنا ان زيادة عدد الباكيتات الملتقطة ربما يؤدي الى اكتشاف البرامج التي تجمع الباكيتات من قبل أنظمة WIDS.



الشكل (٥-٩) يبن عدد البلاكيتات اللازمة لكسر الشيفرة في السيناريوهات المدروسة

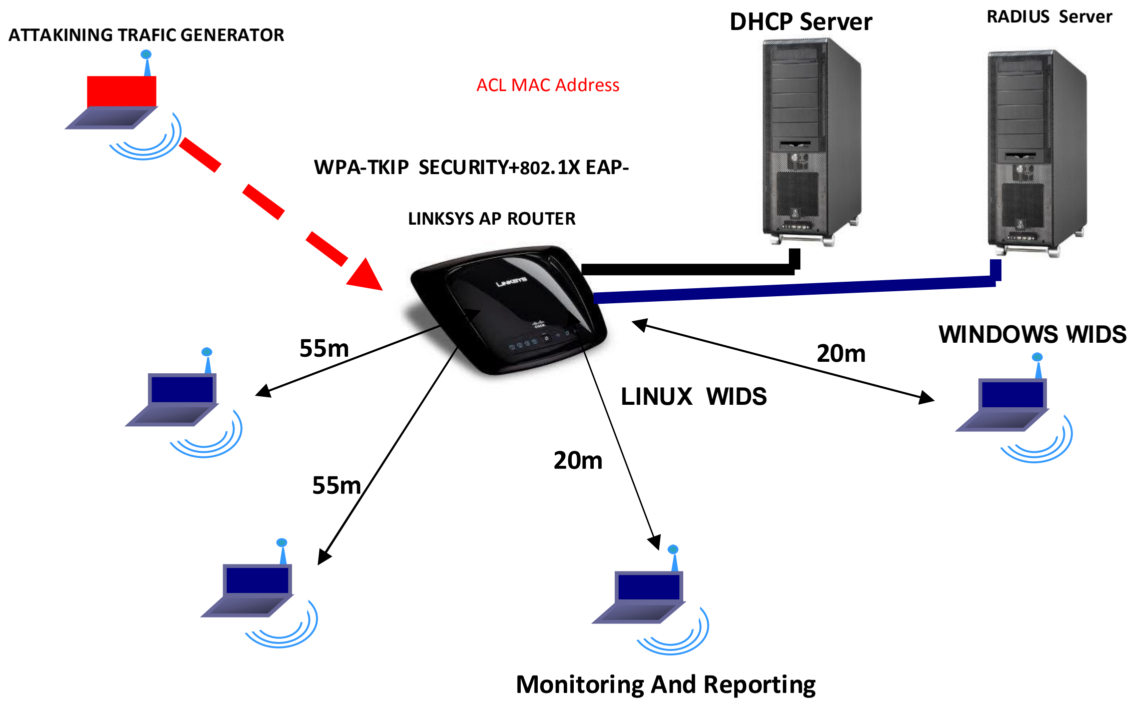


الشكل (٥-١٠) يبن عدد البلاكيتات اللازمة لكسر الشيفرة في السيناريوهات المدروسة

٣-٦-٢-١ دراسة تأثير لوائح التحكم بالوصول (ACL) على البارامترات الأمنية

◄ السيناريو السادس S6 : يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٤-٦) الهدف من هذا السيناريو اختبار نقطة الهدف منه اختبار نقطة الوصول مع مخدم RADIUS و DNS DHCP مع نظام تشفير WPA TKIP 128BIT واستخدام المعيار 802.1X

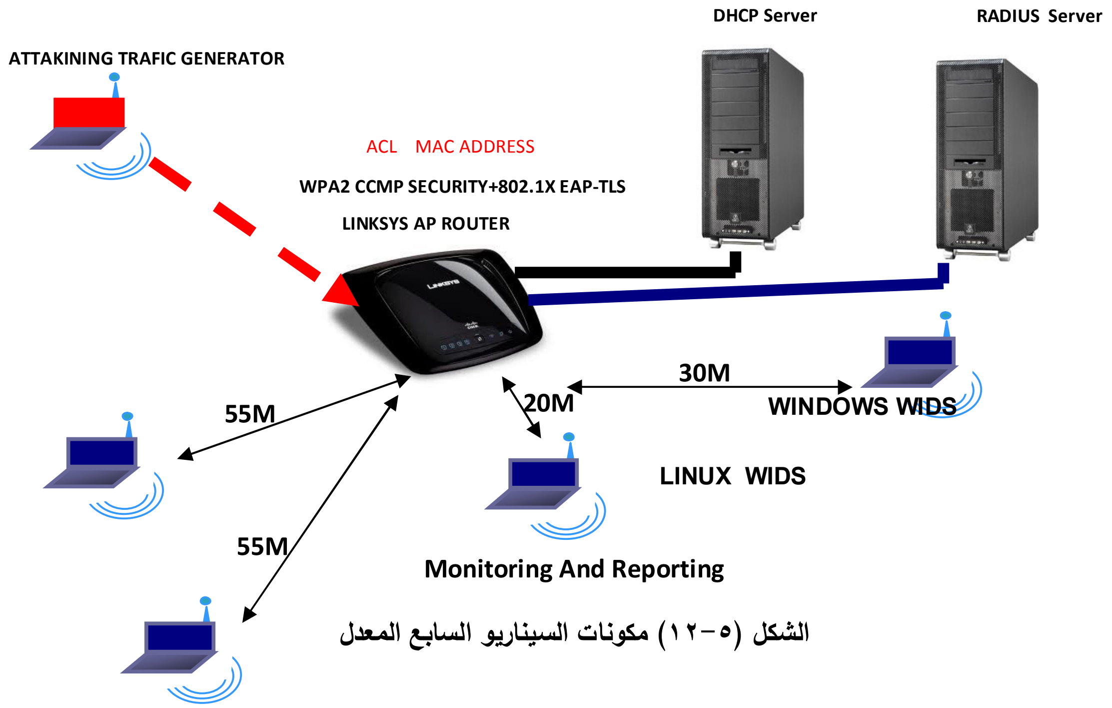
◄ السيناريو السادس المعدل S66 : الهدف منه اختبار نقطة الوصول مع مخدم RADIUS و DHCPداخلي مع نظام تشفير WPA TKIP 128BIT واستخدام المعيار 802.1X ولوائح التحكم بالوصول ACL والسيناريو مبين بالشكل (٥-١١)



الشكل (٥-١١) مكونات السيناريو السادس المعدل

◀ السيناريو السابع S7 : يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٤-٧) الهدف من هذا السيناريو اختبار نقطة الهدف منه اختبار نقطة الوصول مع مخدم RADIUS و DNS DHCP مع نظام تشفير WPA2-CCMP 128BIT واستخدام المعيار 802.1X مع ACL

◀ السيناريو السابع المعدل S7٧ : يعتمد هذا السيناريو على التشكيلة الأمنية المبينة في الشكل (٥-١٣)
الهدف من هذا السيناريو الهدف منه اختبار نقطة الوصول مع مخدم RADIUS و DHCPداخلي مع نظام تشفير WPA2-CCMP 128BIT واستخدام المعيار 802.1X مع ACL



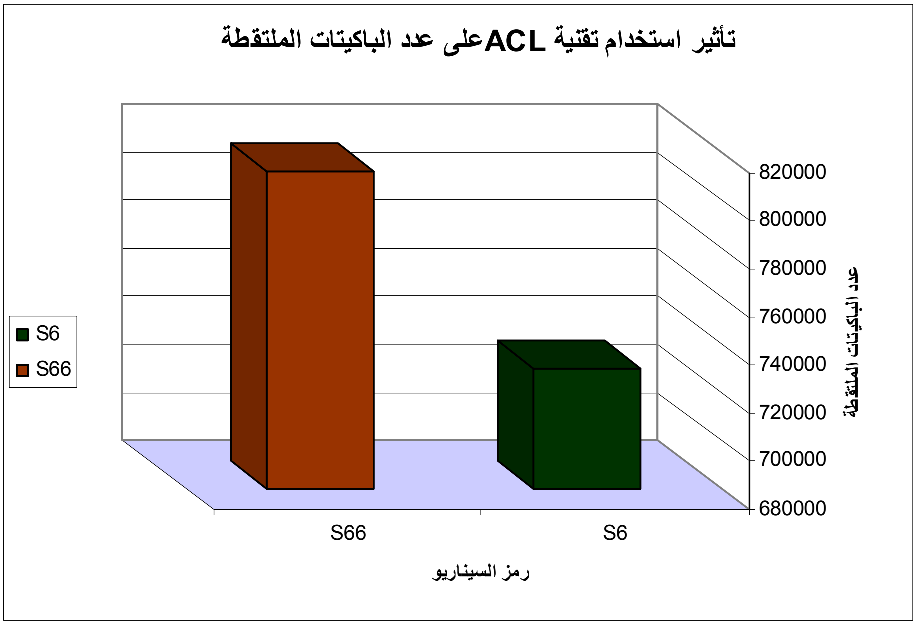
الشكل (٥-١٢) مكونات السيناريو السابع المعدل

يبن الجدول (٥-٦) نتائج اضافة لوائح تحكم بالوصول الى السيناريوهات المدروسة وتأثر باقي البارامترات بذلك

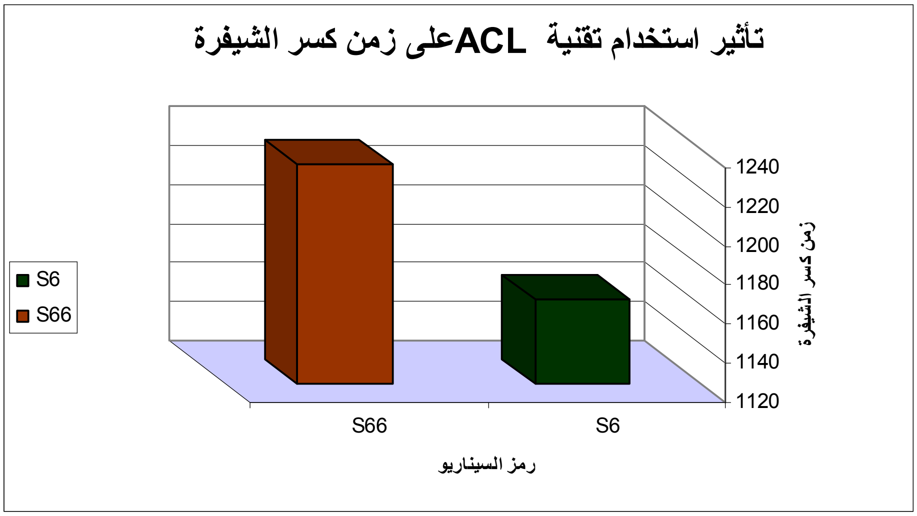
Scenario NO.	Scenario Description	Authenication Time in Seconds A	NO. OF Autentication messages M	TCP through put in Kbps T	Cracking Time C	NO OF Packets
S6	**Wpa802.1x** + DHCP **+RADIUS+wc1+wc2**	**0.163621**	**25**	**11518**	١١٦٣	٧٣٠٠٠٠
S66	**Wpa802.1x** + DHCP **+RADIUS+wc1+wc2+ACL**	**٠.195422**	**25**	**11518**	١٢٣٣	٨١٢٠٠٠
S7	**Wpa2 -802.1x+** DHCP **++RADIUS +wc1 +wc2**	**٠.212345**	٢٨	**10366**	-	-
S77	**Wpa2 -802.1x+** DHCP **++RADIUS +wc1 +wc2+ACL**	**٠.253944**	٢٨	**10366**	-	-

الجدول (٥-٦) قيم بارامترات السيناريوهات المدروسة بعد اضافة ACL

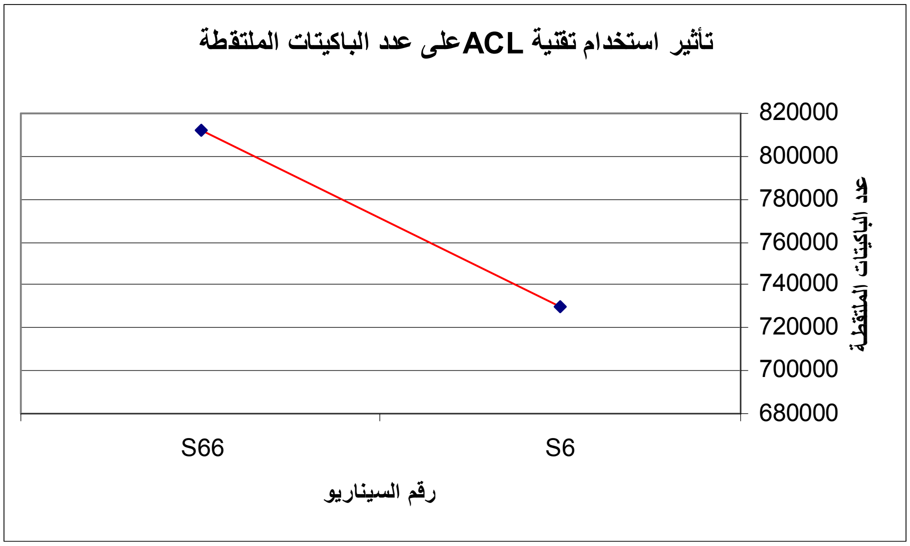
نلاحظ من الجدول (٥-٦) ان اضافة لائحة تحكم بالوصول لنقطة الوصول AP ادى الى زيادة طفيفة في زمن المصادقة وبالتالي زمن الوصول نتيجة لاضافة زمن للبحث عن العناوين MAC في قاعدة بيانات نقطة الوصول و لم يؤثر اضافة هذه اللوائح على البارامترات الاخرى للشبكة اللاسلكية مثل عدد رسائل المصادقة و زمن المصادقة والانتاجية و لكن التأثير ظهر في زمن كسر الشيفرة و عدد الباكيتات الازم التقاطها لكسر الشيفرة مما يعني ان هذه الطريقة ربما تكون فعالة في زيادة امن الشبكة ولكن لتجاوز جانبها السلبي في زيادة الأزمنة يجب ة تطوير طرق البحث في قاعدة بيانات نقطة الوصول لتصبح أكثر سرعة .وهذا مبين في الأشكال (٥-١٣)و(٥-١٤)و(٥-١٥)و(٥-١٦)



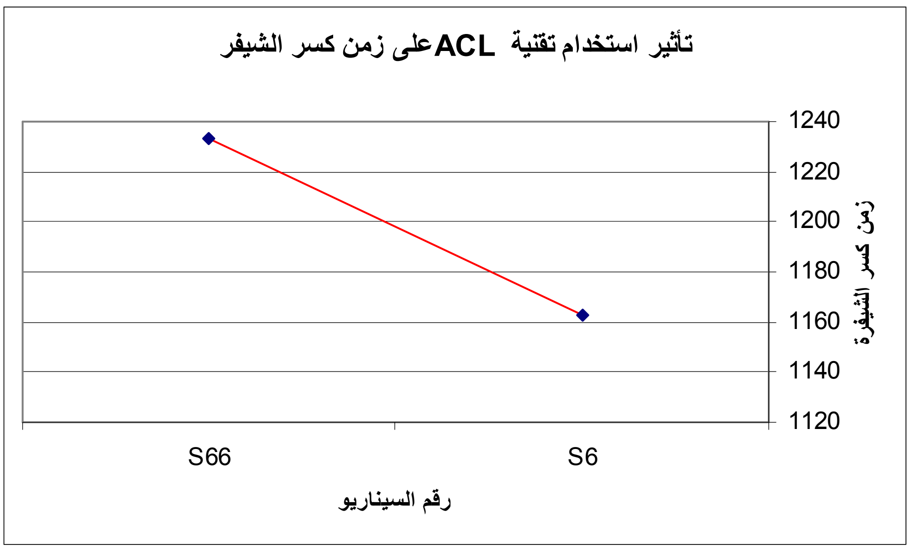
الشكل (٥-١٣) يبن مقارنة بين استخدام تقنية ACL على عدد الباكيتات الملتقطة



الشكل (٥-١٤) يبن مقارنة بين استخدام تقنية ACL على على زمن كسر الشيفرة



الشكل (٥-١٥) يبن مقارنة بين استخدام تقنية ACL على عدد الباكيتات الملتقطة



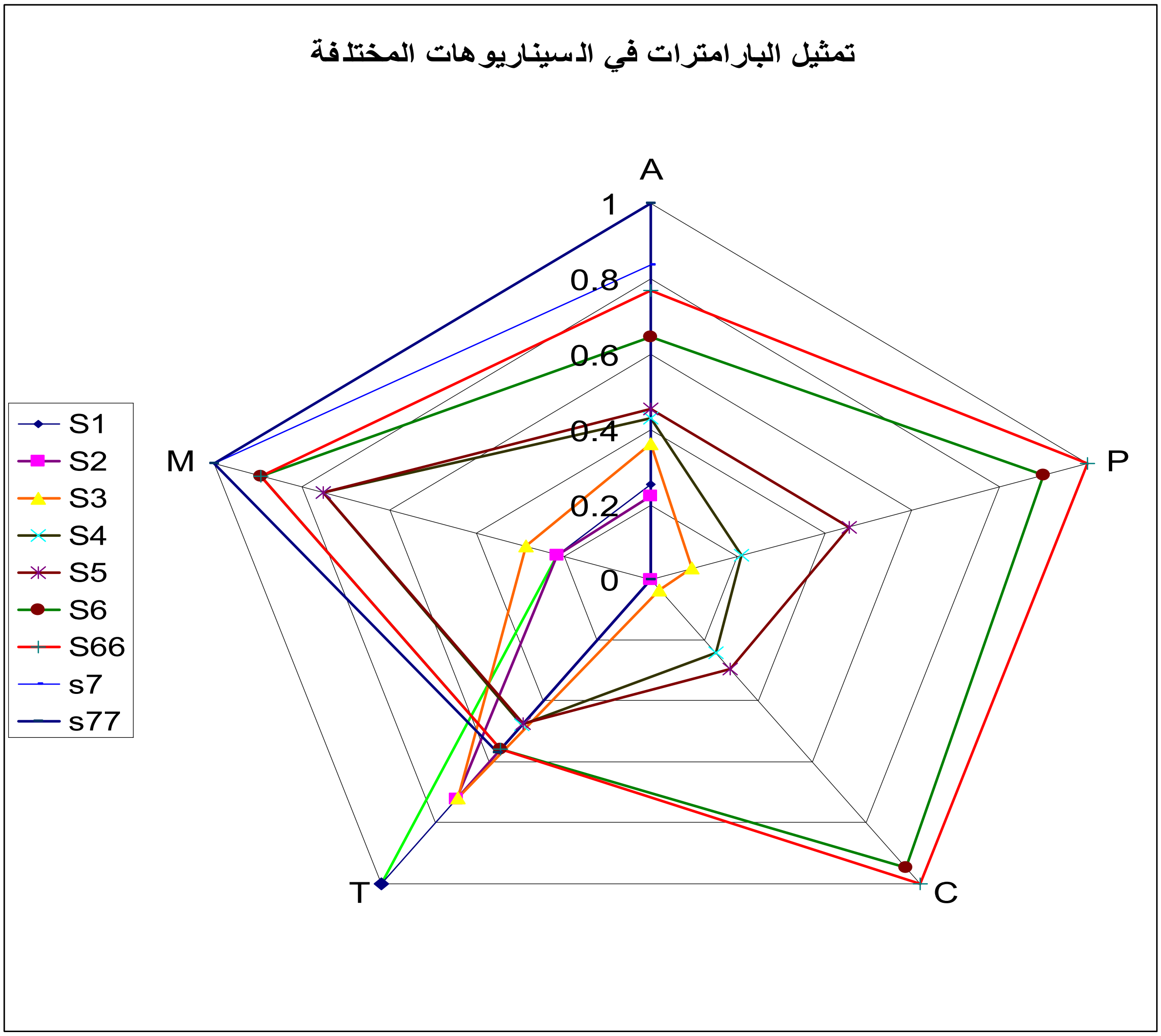
الشكل (٥-١٦) يبن مقارنة بين استخدام تقنية ACL على على زمن كسر الشيفرة

بعد إنجاز القياسات السابقة تم جمع النتائج لجميع البارامترات ضمن الجدول (٥-٧)

Scenario NO.	Scenario Description	Autentication Time in Seconds A	NO. OF Autentication messages M	TCP throughput in Kbps T	Cracking Time C	NO OF Packets
١	Open System +DNS DHCP+WC1	**0.064283**	٦	**20705**	–	–
٢	Open System + DNS DHCP +wc1+wc2	**0.056324**	٦	١٤٨٩٣	–	–
٣	Wep+ DNS DHCP +wc1+wc2	**0.091875**	**8**	١٤٨٤٩	**42**	**78000**
٤	Wep802.1x+ DNS DHCP +RADIUS+wc1+wc2	**0.109325**	**21**	٩٨١٩	٢97	**167000**
٥	Wep128-802.1x+ DNS DHCP +RADIUS+wc1+wc2	**0.115243**	**21**	٩٧٤٦	٣36	**368000**
٦	Wpa802.1x + DNS DHCP +RADIUS+wc1+wc2	**0.163621**	**25**	**11518**	**1163**	**730000**
S66	**Wpa802.1x** DNS DHCP **+RADIUS+wc1+wc2+ ACL**	**.195422٠**	**25**	**11518**	١٢٣٣	٨١٢٠٠٠
٧	Wpa2 -802.1x+ DNS DHCP ++RADIUS +wc1 +wc2	**٠.212345**	٢٨	**11766**	–	–
S77	**Wpa2 -802.1x+** DNS DHCP **+RADIUS +wc1 +wc2+ACL**	**٠.253944**	٢٨	**11766**	–	–

الجدول (٥-٧) قيم بارامترات السيناريوهات المختبرة

وتم توليد مخطط عنكبوتي للنتائج في الجدول (٥-٧) وهي مبينة في الشكل (٥-١٧)



الشكل (٥-١٧) مخطط عنكبوتي يبن تمثيل البارامترات والسيناريوهات المدروسة

M= Exchanged Authentication Messages عدد الرسائل المتبادلة

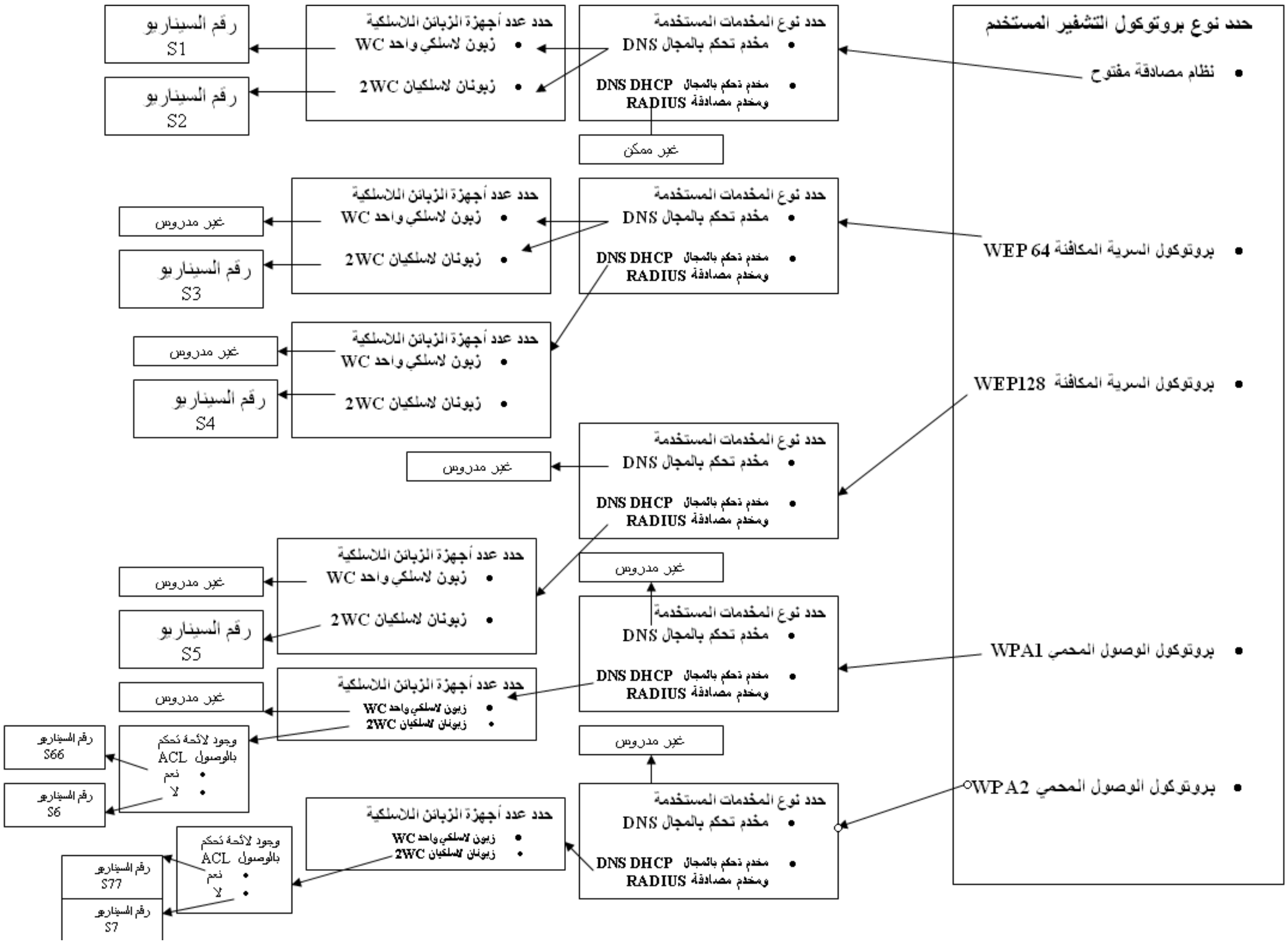
T= Throughpu الإنتاجية

C= Cracking Time زمن كسر الشيفرة

A= Autentication Time زمن المصادقة

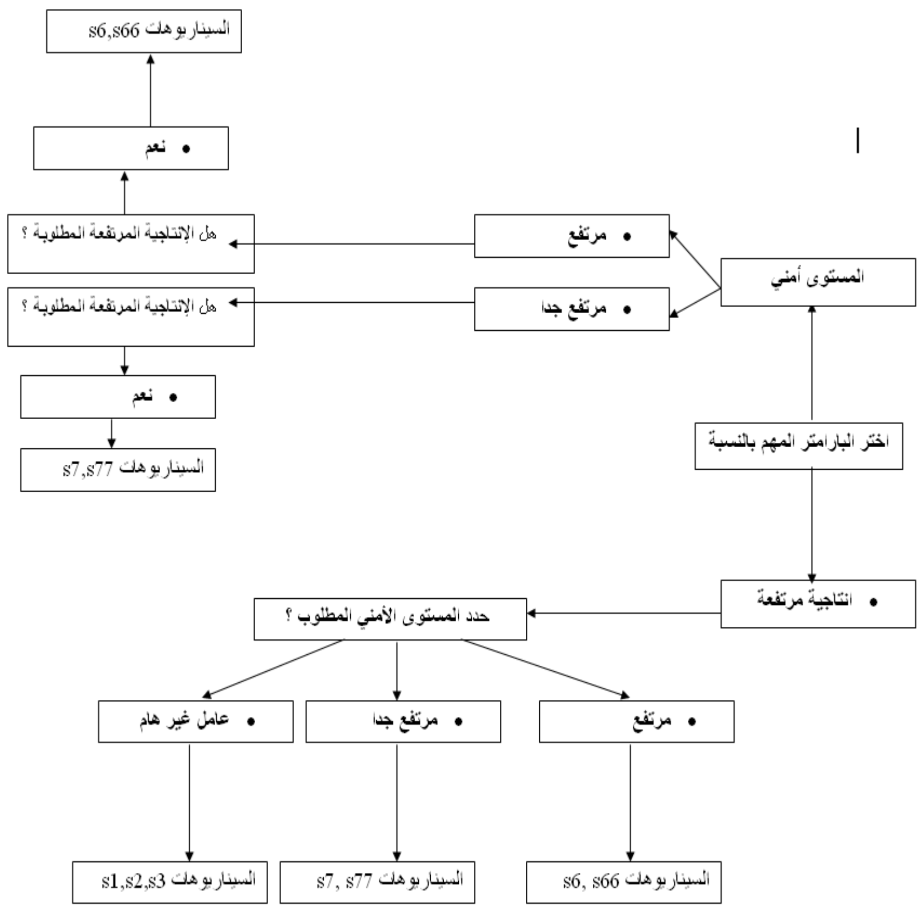
P=Packets No عدد الباكيتات اللازمة لكسر الشيفرة

بالاعتماد على الدراسة السابقة قمنا بتصميم واجهة لاختيار مكونات السيناريوهات وله المخطط الصندوقي المبين في الشكل (٥-١٨) :



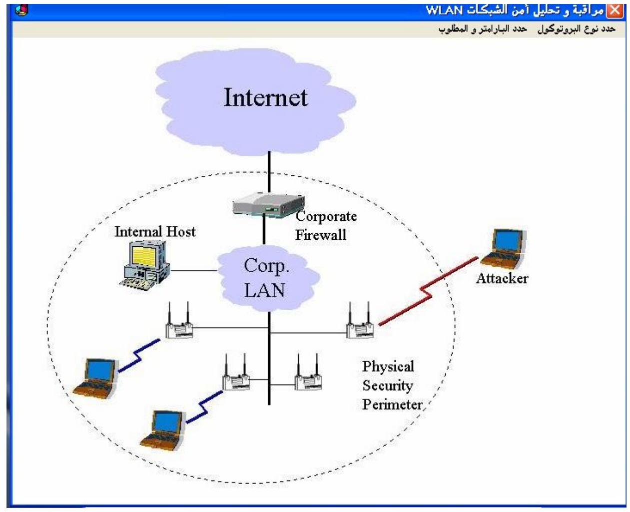
الشكل (٥-١٨) يبن تمثيل البارامترات المدروسة

وقد تم تجميع النتائج حسب المخطط الصندوقي المبين في الشكل (٥-١٩)

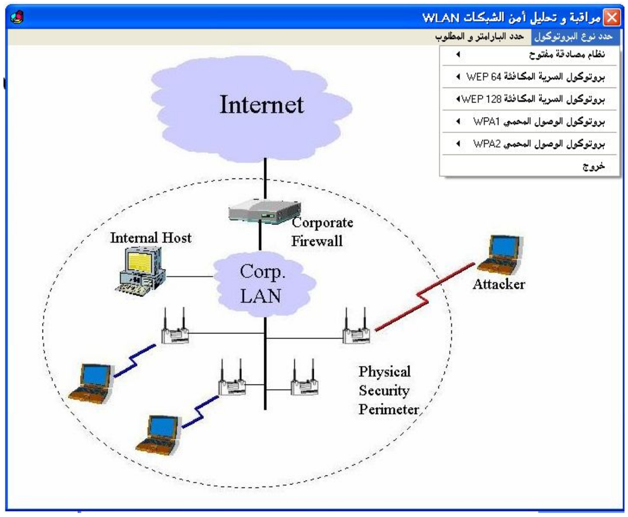


الشكل (٥-١٩) يبن مخطط صندوقي لبرنامج تجميع النتائج

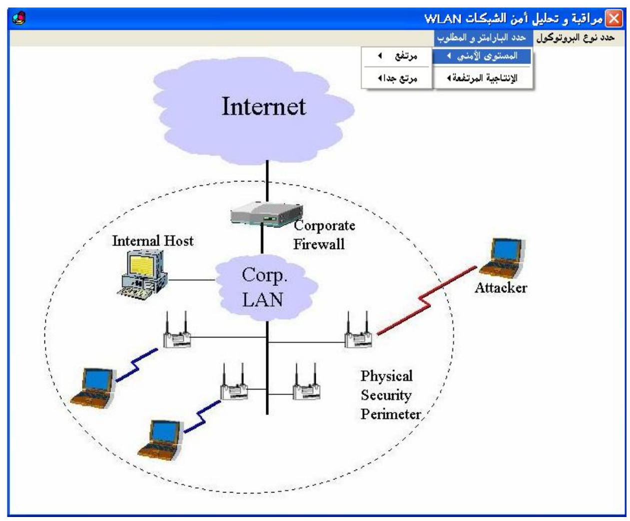
الأشكال (٥-٢٠)و(٥-٢١)و(٥-٢٢)و(٥-٢٣) تبين بعض واجهات البرنامج :



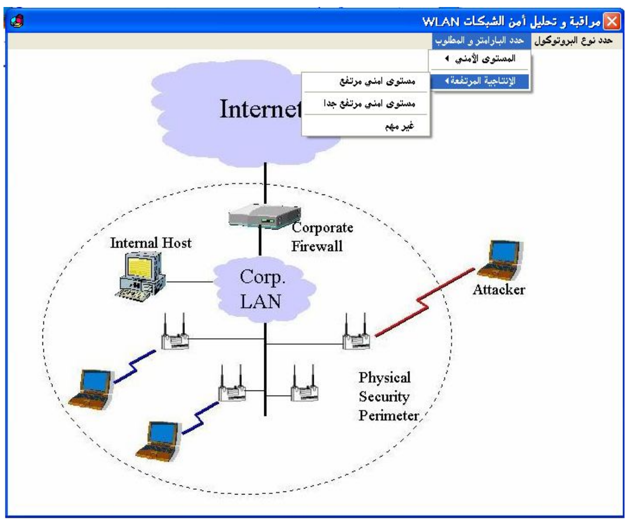
الشكل (٥-٢٠) يبن واجهة البرنامج الرئيسي



الشكل (٥-٢١) يبن واجهة اختيار مكونات السيناريو



الشكل (٥-٢٢) يبن واجهة تجميع النتائج (مستوى أمني)



الشكل (٥-٢٣) يبن واجهة تجميع النتائج (انتاجية)

التوصيات والمقترحات

١. إن الانتقال من نظام أمني بسيط يعتمد على نقطة وصول واحدة مع بروتوكولات تشفير متنوعة إلى نظام أمني أعقد يعتمد على مخدم مصادقة يؤدي الى زيادة صغيرة في أزمنة المصادقة بالمقارنة مع الزيادة الكبيرة التي تطرأ على زمن كسر الشيفرة وذلك في نمط العمل BSS.

٢. لا ينصح باستخدام مخدمات مصادقة في الحالات التي يطلب فيها إنتاجية عالية و إنما البحث عن طرق أخرى لزيادة أمن الشبكات WLAN وفي حالة الاستخدام ينصح بالابتعاد عن بروتوكولات التشفير WEP والاعتماد على بروتوكول WPA مع TKIP,CCMP.

٣. ينصح بتفعيل خدمة لوائح التحكم بالوصول ACL مع بروتوكولات WPA ومع مخدم مصادقة و لا يؤدي ذلك إلى زيادة كبيرة في زمن المصادقة وانما يؤدي إلى زيادة زمن الاختراق أي ممانعة كبيرة للشبكة بسبب اضطرار المهاجم لاستخدام برامج MAC SPOOF ثم كسر التشفير

٤. من تحليل قيم بارامترات شبكة WLAN نجد أن السيناريوهات التي تعتمد على وجود مخدم مصادقة و بروتوكول تشفير WPA1,WPA2 تؤمن مستوى أمني مرتفع مع المحافظة على انتاجية مرتفعة

الملحق رقم ١

جدول بالمصطلحات المستخدمة

Encryption	تشفير
Plaintext	النص الأصلي (المقروء)
Ciphertext	النص المشفر (غير المقروء)
Decryption	التفكيك (عكس التشفير)
Key	مفتاح تشفير
MAC	عنوان فيزيائي
Haking	اختراق
Authentication	مصادقة
Associate	ترابط
Vulnerabilities	عرضة للتهديد
Rogue access points	نقاط وصول مشبوهة
War Driving	ملتقطي الاشارة اللاسلكية
Supplicant	زبون لاسلكي
Troughput	الانتاجية
Beacon	مرشد لاسلكي
Client	زبون
Probing	سبر
Active	فعال (نشط)
Passive	خامل
Spoof	انتحال
Monitorring	مراقبة
Link Layer	طبقة وصل البيانات
Transport Layer	طبقة النقل
Firewall	جدار النار
Network Layer	طبقة الشبكة

الملحق رقم ٢

جدول بالمختصرات المستخدمة

wlan	Wireless LAN
IDS	Intrusion Detection System
DOS	Denial Of Service
VPN	Virtual Private Network
WPA	Wifi Protected Access
WEP	Wired Equivalnt Privcy
WiFi	Wireless Fidelity
EAP	Extensible Authentication Protocol
TKIP	Temporary Key Integrity Protocol
CCMP	CTR with CBC-MAC Protocol
SSID	Service Set Identifier
BSSID	Basic Service Set Identifier
IBSS	Independent Basic Service Set
RADIUS	Remote Authentication Dial-in User Service
AES	Advanced Encryption System
ESS	Extended Service Set
TLS	Transport Layer Security
ACL	Access Control List
IEEE	Institute Of Electrical and Electronic Engineers
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
EAPON	Extensible Authentication Protocol over LAN
BSS	Basic Service Set
MAC	Media Access Control
OUI	Organizationally Unique Identifier
ARP	Address Resolution Protocol
RSN	Robust Security Networks
RF	Radio Frequency
PSK	Pre Shared Key

الملحق رقم ٣

جزء من الكود البرمجي لبرنامج تجميع النتائج

```
Option Explicit
Private Sub aman1_Click()
End Sub
Private Sub aman21_Click()
RunMyExcel 7
End Sub
Private Sub aman9_Click()
RunMyExcel 6
End Sub
Public Sub RunMyExcel(ByVal Index As Integer)
Dim F As String
Dim A As String
Dim C As String
Dim W As String
Dim Ta As String
Select Case Index
   Case 1
   W = "c:\S1.xls"
   Case 2
   W = "c:\S2.xls"
   Case 3
   W = "c:\S3.xls"
   Case 4
   W = "c:\S4.xls"
   Case 5
   W = "c:\S5.xls"
```

```
    Case 6
   W = "c:\S6.xls"
    Case 66
    W = "c:\S66.xls"
    Case 7
    W = "c:\S7.xls"
    Case 77
    W = "c:\S77.xls"
    Case 8
    Case 9
    Case Else
    MsgBox "No Result"
    Exit Sub
End Select
If Dir(A) = "" Then
    MsgBox " ÇáãáÝ ÇáãØáæÈ ÛíÑ ãæÌæÏ", vbMsgBoxRight + vbCritical
    Exit Sub
End If
If Dir("C:\Program Files\Microsoft Office\Office12\Excel.Exe") = "" Then
    If Dir("C:\Program Files\Microsoft Office\OFFICE11\Excel.Exe") = "" Then
        MsgBox " ÇáãáÝ ÇáãØáæÈ ÛíÑ ãæÌæÏ", vbMsgBoxRight + vbCritical
        Exit Sub
    Else
        Ta = "C:\Program Files\Microsoft Office\OFFICE11\Excel.Exe"
    End If
Else
    Ta = "C:\Program Files\Microsoft Office\Office12\Excel.Exe"
```

```
End If
A = Chr(34) + Ta + Chr(34)
F = Chr(34) + W + Chr(34)
C = A & " " & F
Dim S As Long
S = Shell(C, vbNormalFocus)
End Sub
Private Sub Cro1_Click()
MsgBox "ÛíÑ ãÏÑæÓ", vbMsgBoxRight + vbCritical
End Sub
Private Sub dro10_Click()
MsgBox "ÛíÑ ãÏÑæÓ", vbMsgBoxRight + vbCritical
End Sub
Private Sub ero1_Click()
MsgBox "ÛíÑ ãÏÑæÓ", vbMsgBoxRight + vbCritical
End Sub
Private Sub Kro2_Click()
MsgBox "ÛíÑ ãäßäÉ", vbMsgBoxRight + vbCritical
End Sub
Private Sub Mro4_Click()
MsgBox "ÛíÑ ãÏÑæÓ", vbMsgBoxRight + vbCritical
End Sub
Private Sub mro5_Click()
RunMyExcel 3
End Sub
Private Sub Pro4_Click()
End Sub
```

```
Private Sub Qro1_Click()
RunMyExcel 66
End Sub
Private Sub Qro2_Click()
RunMyExcel 6
End Sub
Private Sub salam3_Click()
RunMyExcel 7
End Sub
Private Sub salam5_Click()
RunMyExcel 1
End Sub
Private Sub salam6_Click()
RunMyExcel 6
End Sub
Private Sub Tro1_Click()
MsgBox "ÛíÑ ãÏÑæÓ", vbMsgBoxRight + vbCritical
End Sub
Private Sub vro1_Click()
RunMyExcel 77
End Sub
Private Sub vro2_Click()
RunMyExcel 7
End Sub
Private Sub wro1_Click()
MsgBox "ÛíÑ ãÏÑæÓ", vbMsgBoxRight + vbCritical
End Sub
```

```
Private Sub Wro2_Click()

RunMyExcel 4

End Sub

Private Sub yro1_Click()

MsgBox "ÛíÑ ãÏÑæÓ", vbMsgBoxRight + vbCritical

End Sub

Private Sub yro2_Click()

RunMyExcel 5

End Sub

Private Sub Zro1_Click()

RunMyExcel 1

End Sub

Private Sub zro2_Click()

RunMyExcel 2

End Sub
```


الملحق رقم 4

Bibliography

المراجع العربية والأجنبية

1 – Nilufar Baghaei., IEEE 802.11 Wireless LAN Security Performances Using Multiple ClientsUniversity of Canterbury, Christchurch, New Zealand ,2007

2- Jorgen Ellingson .,Layers One &Two of 802.11 WLAN Security, SANS Institute InfoSec Reading Room,u k, 2001

3- Min-kyu Choi1), Rosslin John Robles1), Chang-hwa Hong2).Wireless Network SecurityVulnerabilities, Threats and Countermeasures, Tai-hoon Kim1
School of Multimedia, Hannam University, Daejeon, Korea, 2008

٤ – Craig Valli., Wireless Snort – A WIDS in progress, Edith Cowan University, Western Australia, 2004

٥ – Joshua Wright., Detecting Detectors: Layer 2 Wireless Intrusion Analysis sans pub, 2004

6-Ignacio Porres Ruiz del Mar Fernández de Ramón. An evaluation of current IDSMaría Linköping, February 7th, 2008

7- S.cunningham,Peace Driving: Case Studies of Wi-Fi Usage , Centre for Applied Internet Research, Glyndŵr University, Wrexham –UK, 2009

8- Gianluca Papaleo. Wireless Network Intrusion Detection System: implementation and architectural issues , Università degli Studi di Genova ,2006

9- GILBER H., Securing Wireless LANs, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England ,2003

10- Turbo Access Control Lists. http://newsroom.cisco.com/dlls/index.html sited on 18-2-2011

11- Luis Carlos Wong, An Overview of 802.11 Wireless Network Security Standards & Mechanisms, GIAC Security Essentials Certification (GSEC)October 2004

12-Sangram Gayal Dr. S. A. Vetha Manickam Wireless LAN Security Center for Information and Network Security, Pune University, 2006

13- ضاهر, رياض, أساسيات شبكات الحاسوب , جامعة تشرين, 2011

14- Scott F. Midkiff, Chair Luiz A. DaSilva Amir Zaghlou, Analyzing Wireless LAN Security Overhead, Falls Church, Virginia, April 17, 2006

15-D.S. Dawoud, R.NGOGA Said, P. Dawoud, Measuring Performance impact of Authentication and Encryption protocols on a Wireless LAN, University of UKZN 2007

16-Communications Security Establishment Canada, 802.11 Wireless LAN Vulnerability Assessment, May 2009

17- Jeffrey Wheat Randy Hiser Jackie Tucker Alicia Neely, Designing a Wireless Network, Copyright © 2001 by Syngress Publishing, Inc.USA

18- M.Fattouche and H.Zaghloul, " Methode and apparatus for multiple access between transceivers in wireless communication using OFDM spread spectrum, "US. Patent no. 5,282,222Jan .25, 1994.

19- Q.Ni, "Performance Analysis and Enhancements for IEEE 802.11e Wireless Networks,"IEEE networking magazine, 2005.

20-Y.Xio, "IEEE 802.11n: Enhancements for Higher Throughput in WLANs,"IEEE Wirless Communication Magazine, 2005.

21- Gilbert Held, Securing Wireless Lans, John wiely & Sons Ltd .2003

22-Barken, L.,How Secure is Your Wireless Network? Safegurding your Wifi LAN, First Edition , Prentice Hall PTR , Upper Saddle River , NJ,USA ,2003 .